Networking Configuration Guide

BCM50 2.0

Business Communications Manager

Document Status: **Standard**

Document Number: **NN40020-603**

Document Version: **01.08**

Date: **May 2008**

NORTEL

Copyright © 2008 Nortel Networks. All Rights Reserved

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Contents 3

List of procedures 19

Chapter 1
Getting started with BCM 25

About this guide 25
Purpose 25
Audience 25
Acronyms 26
Organization 26
About BCM 26
Symbols and conventions used in this guide 28
Related publications 29
How to get Help 31
Getting Help from the Nortel Web site 31
Getting Help over the telephone from a Nortel Solutions Center 31
Getting Help through a Nortel distributor or reseller 32

Chapter 2
System telephony networking overview 33

Basic system configurations 33
Tandem calling to a remote PSTN 36
Private network parameters 37
Lines used for networking 39
Types of private networks 39
Routing-based networks using T1 E&M lines 40
PRI networking using Call-by-Call services 41
PRI SL-1/Q.Sig/DPNSS and VoIP trunk networking 42
System dialing plans 43
Creating tandem private networks 43
Understanding Nortel Voice Networking (MCDN) network features 46
Network Call Redirection Information 46
ISDN Call Connection Limitation 47
Trunk Route Optimization 48
Trunk Anti-tromboning 49
Networking with ETSI QSIG 50
ETSI Euro network services 51
DPNSS 1 services 52
DPNSS 1 capabilities 53

DPNSS 1 features 53
Private networking with DPNSS 60
BRI Euro Protocol 61
Naming convention 62
Application level differences 62
Protocol level differences 62

Chapter 3
Telephony programming: Configuring call traffic 63

Incoming calls 66
Outgoing calls 70

Chapter 4
Application Resources overview 73

Types of resources 73
Total and Reserved Resources 73
Setting values for application resources 74

Chapter 5
Application Resources panel 77

Chapter 6
Module configuration: Trunk modules. 81

Configuring the trunk module parameters 83
Module parameters list 83

Chapter 7
Managing modules. 87

Disabling or enabling a bus or module 87
Disabling or enabling a port channel setting 87
Trunk module metrics 88

Chapter 8
Lines overview 89

Understanding how the system identifies lines 90
Determining which lines you need to program 90
BRI loops programming 92
Line record 93
Line characteristics 93
Line restrictions 93
Remote restrictions 94
Voice message center 94
Line Job Aids 94
Determining line numbers and destination codes 95

Line pool tips 96
Using loss packages 97
Turn Privacy on or off for a call 98
Programming line access 98
Making lines available 98
Incoming calls 99
Outgoing calls 99

Chapter 9
Configuring telephony resources. 101

Telephony Resources table 102
Media bay module panels 104
Trunk Module Parameters 104
Call-by-Call Service Selection 108
Port details 110
Provisioning module lines/loops 112
IP telephones 112
IP Terminal Global Settings 113
IP telephone set details 114
Voice over IP trunks 115
Routing table 116
H323 Settings 118
H323 Media Parameters 122
SIP Settings 125
SIP Media Parameters 126
SIP URI Map 127

Chapter 10
Configuring lines 129

Trunk/Line data, main panel 130
Properties 132
Preferences (lines) 134
Restrictions (Line and Remote) 137
Assigned DNs 138

Chapter 11
Configuring lines: Target lines 141

Configuring Target line settings 144

Chapter 12
Configuring lines: PRI 145

Configuring PRI line features 147
Configuring PRI Call-by-Call services 148

Chapter 13
Configuring lines: T1-E&M 151
Configuring E&M line features 155

Chapter 14
Configuring lines: T1-Loop start 157
Configuring digital (T1/E1) loop start lines 161

Chapter 15
Configuring lines: T1-Digital Ground Start 163
Configuring digital ground start line features 166

Chapter 16
Configuring lines: T1-DID 169
Configuring DID line features 172

Chapter 17
Configuring lines: DASS2 lines 175
Configuring DASS2 line features 177

Chapter 18
Configuring lines: DPNSS lines 181
Configuring DPNSS line features 183

Chapter 19
BRI ISDN: BRI loop properties 187
Configure loop type and general parameters 188
T-loop general settings 189
T-loop SPIDS and network DNs 190
T-loops D-packet service 192
S-loops assigned DNs 193

Chapter 20
BRI ISDN: BRI T-loops 195
Configuring BRI T-loop parameters 197
Configuring BRI lines 197

Chapter 21
Programming BRI S-loops, lines, and ISDN devices 201
Setting BRI properties for ISDN device connections 201
DN records: ISDN devices 202
Configuring an ISDN telephone DN record 204

Chapter 22
Configuring CLID on your system 205

Programming incoming CLID 207
Using alpha tagging for name display (incoming) 207
Programming outgoing CLID 208

Chapter 23
CLID: Name display 211

Business name display 212
Alpha tagging for name display 212
Name display 213
Incoming and outgoing call display 214

Chapter 24
Dialing plans. 217

Creating dialing plans 218
Public and Private Received numbers 221
Private network dialing 221
Setting up public network dialing 221
Outgoing call routing 222
Incoming call routing 224
Processing incoming calls 225
Determining line access dialing 228
Understanding access codes 229
Call Park codes 230
Creating Direct Dial sets 231
Tips about access codes 232
Using the MCDN access codes (tandem calls) 232
Line pool access codes 234
Using Carrier codes 234
Configuring call routing 234
Configuring Call-by-Call services 235
Call-by-Call services 236
Switches supporting Call-by-call limits 237
Provisioning for Call-by-Call limits with PRI 238
Call-by-Call service routing 238
PRI routing protocols 239
Using destination codes 239
Why use destination codes? 240
Deciding on a code 241
Adding Carrier access codes to destination codes 242
Routing schedules and alternate routes 243

Setting up VoIP trunks for fallback 244

Chapter 25
Dialing plan: Routing configurations 247

Destination code numbering in a network 249
Setting up a destination for local calling 249
Setting up a route through a dedicated trunk 250
Grouping destination codes using a wild card 251
Programming for least-cost routing 252
Using multiple routes and overflow routing 252
Dialing plan using public lines 254
Programming the PRI routing table 255
Adding Carrier access codes to destination codes 256
Using the MCDN access codes to tandem calls 257

Chapter 26
Dialing plan: Routing and destination codes 259

Routes 260
Destination codes 262
Alternate routes for routing schedules 264
Second Dial Tone 265

Chapter 27
Dialing plan: System settings 267

Common dialing plan settings 267
DN length constraints 270
Received number notes 271
Tips about access codes 272
Call Park codes 273

Chapter 28
Dialing plan: Public network 275

Public dialing plan settings 275
Public Network Settings 276
Public network DN lengths 277
Carrier Codes 279

Chapter 29
Dialing plan: Private network settings 281

Private Network dialing plan settings 281
Private Network Settings 282
Private Network - MCDN network (PRI SL-1, PRI ETSI, VoIP) 284
VoIP-specific private network dialing 285

ETSI-specific network features 286
Outgoing private calls routing 287

Chapter 30
Public networking: Setting up basic systems 289

Public networks: PBX system setup 289
Public network: DID system 290

Chapter 31
Public networking: Tandem calls from private node 293

Programming for tandem dialing 293
Caller access on a tandem network 294

Chapter 32
Private networking: MCDN over PRI and VoIP 297

Using MCDN to network with a Meridian system 297
Meridian system requirements 297
Meridian MCDN call features over PRI SL-1 lines 299
MCDN networking checklist 303
UDP-specific programming 304
CDP-specific programming 305
VM programming with Meridian 1 306
Meridian TRO programming 307
An example of a private network with Meridian 1 307
Configuring fallback over a VoIP MCDN network 311
MCDN functionality on fallback PRI lines 312
Networking with ETSI QSIG 313

Chapter 33
Private networking: Basic parameters 315

Private networking protocols 315
Keycode requirements 315
Remote access to the network 316
Other programming that affects private networking 316
Types of private networks 316

Chapter 34
Private networking: MCDN and ETSI network features 319

Configuring MCDN network features 319
Configuring ETSI Euro network services 321

Chapter 35
Private networking: PRI and VoIP tandem networks 323

Routing for tandem networks 323
Routing calls through a tandem network 324
Calls originating from the public network 325
Calls originating in the private network 326
Using VoIP to tandem systems 327

Chapter 36
Private networking: DPNSS network services (UK only) 331

Using the diversion feature 331
Using the Redirection feature 333
Executive intrusion, Intrusion protection level 333
Call offer 334
Route Optimization 335
Loop avoidance 335
Private networking with DPNSS 335

Chapter 37
Private networking: Using destination codes 339

Chapter 38
Private networking: PRI Call-by-Call services. 343

Chapter 39
Configuring voice messaging. 347

Centralized Voice Messaging (external voice mail) 347
Programming MWI and MWC strings 348
Local voice messaging access (CallPilot Manager) 349

Chapter 40
Configuring centralized voice mail. 351

Local system as host 351
Meridian system as host 352
System set up for host system 352
System set up for satellite systems 353
Configuring the system for centralized voice mail 355

Chapter 41
Dialing plan: Line pools and line pool codes 357

Line pools (and access codes) 357
Line pools: DNs tab 359
Line pools: Call-by-Call Limits tab (PRI only) 360

Chapter 42
VoIP overview 363

IP telephones 363
VoIP trunks 363
Creating an IP telephony network 363
Telephones 364
Gatekeepers 364
SIP Proxy 364
IP Network 364
Key VoIP concepts 365

Chapter 43
VoIP trunk gateways 367

Pre-installation system requirements 367
How VoIP trunks make a network 368
Local gateway programming 369
Routing Table 370
PSTN call to remote node 371
Fallback to PSTN from VoIP trunks 373
Describing a fallback network 374
How fallback routing works 375
Optional VoIP trunk configurations 377
Gatekeeper call scenarios 378
Operational notes and restrictions 379

Chapter 44
Configuring VoIP trunk gateways 381

Configuring VoIP trunk media parameters 382
Setting up the local gateway 383
Setting up remote gateways 385
Configuring a remote gateway (H.323 trunks) 385
Configuring VoIP lines 385
Configuring VoIP line features 386

Chapter 45
VoIP interoperability: Gatekeeper configuration 389

Using CS 1000 as a gatekeeper 389
CS 1000 configuration 390

Chapter 46
Setting up VoIP trunks for fallback 391

Configuring routes for fallback 391
Activating the VoIP schedule for fallback 395

Deactivating the VoIP schedule 396
Example: A private network configured for fallback 396

Chapter 47
T.38 fax 401

Enabling T.38 fax 401
Lines 402
Media gateways 402
T.38 Fax restrictions 403
Operational notes and restrictions 403

Chapter 48
Port ranges overview. 405

RTP over UDP 405
UDP 405
Signaling Ports 405

Chapter 49
Port Ranges panel 407

RTP over UDP Port Ranges 407
Adding new RTP over UDP Port Ranges 408
Deleting RTP over UDP Port Ranges 408
Modifying RTP over UDP Port Ranges 409
UDP Port Ranges 409
Signaling Port Ranges 410

Chapter 50
Media gateways overview 411

Chapter 51
Media Gateways panel. 413

Chapter 52
Call security and remote access 415

Defining restriction filters 415
Notes about restriction filters 416
Default filters (North America) 417
Default filters (other) 418
Restriction filter examples 418
Remote call-in programming 419
Creating Direct Inward System Access (DISA) 420
Defining remote access packages 422
Defining CoS passwords 423
External access tones 425

Chapter 53
Call Security: Configuring Direct Inward System Access (DISA) 427

Remote access overview 427
Setting up remote access on lines 430
Remote access on loop-start trunks 430
Remote access on T1 DID trunks 430

Chapter 54
Call security: Restriction filters 433

Restriction filters 433
Adding a restriction filter and exceptions 435
Default filters 436

Chapter 55
Call security: Remote access packages 439

Configuring remote access packages 439

Chapter 56
Configuring CoS passwords for remote access 443

Class of Service table 443
Adding or modifying a CoS password values 444
External access tones 447

Chapter 57
LAN overview 449

What is a LAN? 449
LAN settings 449
DHCP configuration 449

Chapter 58
Configuring the BCM with a DHCP address 451

Chapter 59
Data networking overview 453

What is data networking? 453
About the BCM VoIP capability 453
Network routing 453
Configuring the BCM with data networks 453

Chapter 60
IP Subsystem 455

Main panel tabs: General settings 455
IP settings options 455
DNS Settings options 456

MTU option 456
Main panel tabs: Internal subnets 458
Internal Subnet settings 458
Internal Subnet Details 459
Main panel tabs: Dial-out Static Routes 461
Configuring static routes 463

Chapter 61
Data network prerequisites checklist. 465

Network diagram 465
Network devices 466
Network assessment 466
Keycodes 467
System configuration for IP telephony functions 467
VoIP trunks 468
IP telephone records 468

Chapter 62
Router overview 469

ADSL and Ethernet configurations 469
Router features 469

Chapter 63
Router panel 471

Accessing your router 471

Chapter 64
VLAN overview 473

Choosing DHCP for VLAN 473
Specifying the site-specific options for VLAN 474

Chapter 65
DHCP overview. 475

Understanding DHCP 475
DHCP on the BCM 475
Router DHCP Server 475
Main Module DHCP client 476
Main Module DHCP server 476
DHCP network scenarios 476
Default configurations 478

Chapter 66
DHCP Server Settings panel 481

Main panel tabs: General Settings 481
Main panel tabs: IP Terminal DHCP Options 483
Main panel tabs: Address Ranges 486
DHCP subnets 486
Main panel tabs: Lease Info 489

Chapter 67
DHCP configuration with router 491

Changing the default router DHCP configuration 491
Configuring the BCM with a DHCP address 491
Configuring the BCM to act as a DHCP server 491
Determining the status for the DHCP server 492
Using the BCM as a standalone DHCP server 492
DHCP for IP sets 492
Disabling the DHCP server 493

Chapter 68
Firewall configuration resources 495

Chapter 69
Dial Up overview 497

Remote Access Service 498
Automatic Data Dial-Out Service 499
WAN Failover Service 500
Modem compatibility 500

Chapter 70
Dial Up Interfaces panel 501

Dial-out Interfaces panel 501
ISDN interfaces 502
ISDN Dial-out Channel Characteristics 505
ISDN Dial-out Link Parameters 506
ISDN Dial-out IP Address 508
Modem interface 508
Modem Dial-out Link Parameters 510
Modem Dial-out IP Address 512
Global Settings panel 512
WAN failover 513
Modem Dial-In Parameters panel 514
Additional configuration to allow network access functionality 517
ISDN Dial-In Parameters panel 518

Creating an automatic dial-out interface 521
Guidelines for using remote Dial-in 522
Using a dial-up interface as a primary connection 522
Static Routes for Automatic Dial-out Interfaces 524

Appendix A
VPN overview 525

IPSec tunnels 525
IPSec 527
Encryption 527

Appendix B
Silence suppression 529

Silence suppression on half-duplex links 529
Silence suppression on full-duplex links 531
Comfort noise 533

Appendix C
ISDN overview 535

Welcome to ISDN 535
Services and features for ISDN BRI and PRI 537
PRI services and features 538
BRI services and features 538
Service provider features 539
Network name display 539
Name and number blocking (ONN) 540
Call-by-Call Service Selection for PRI 540
Emergency 911 dialing 541
2-way DID 541
Dialing plan and PRI 541
ISDN hardware 542
PRI hardware 542
BRI hardware 542
Clock source for ISDN 544
ISDN BRI NT1 equipment 544
ISDN standards compatibility 545
Planning your ISDN network 545
Ordering ISDN PRI 545
Ordering ISDN BRI 546
Supported ISDN protocols 547

Appendix D

Codec rates 549
Index 551

List of procedures

Contents 3

List of procedures 19

Getting started with BCM 25

System telephony networking overview 33

Telephony programming: Configuring call traffic 63

Application Resources overview 73

Application Resources panel 77

Module configuration: Trunk modules 81
To define the modules to the system....83

Managing modules 87
To enable or disable a bus....87
To turn a port channel on or off....87

Lines overview 89

Configuring telephony resources 101

Configuring lines 129
To add a DN record to a line record....139

Configuring lines: Target lines 141

Configuring lines: PRI 145
To configure Call-by-Call services and the PRI lines....149

Configuring lines: T1-E&M 151

Configuring lines: T1-Loop start 157
To configure digital loop start lines....161

Configuring lines: T1-Digital Ground Start 163
To configure digital Ground Start line features....166

Configuring lines: T1-DID 169
To configure DID line features....172

Configuring lines: DASS2 lines 175

Configuring lines: DPNSS lines 181

BRI ISDN: BRI loop properties 187

BRI ISDN: BRI T-loops 195
To configure BRI T-loop parameters 197
To configure provisioned BRI line features.....198

Programming BRI S-loops, lines, and ISDN devices 201
To set BRI properties for ISDN device connections 202

Configuring CLID on your system 205
To set up alpha tagging on your system.....207
To program the Business Name.....208

CLID: Name display 211

Dialing plans 217

Dialing plan: Routing configurations 247
To build a route to allow local calls.....249
To set up a route through a dedicated trunk.....250
To build a route for a secondary carrier.....252
To set up the multiple routing overflow feature.....253
To program the PRI routing table 255
To program a long distance carrier access code into a destination code.....256

Dialing plan: Routing and destination codes 259

Dialing plan: System settings 267

Dialing plan: Public network 275

Dialing plan: Private network settings 281

Public networking: Setting up basic systems 289

Public networking: Tandem calls from private node 293

Private networking: MCDN over PRI and VoIP 297
To set up the M1 in a BCM network 312
To enable MCDN functionality over PRI fallback lines 312

Private networking: Basic parameters 315

Private networking: MCDN and ETSI network features 319
To configure ICCL 320
To enable TRO 320
To enable TAT.....320
To enable MCID and network diversion 321

Private networking: PRI and VoIP tandem networks 323
To set up a network of BCMs 328

Private networking: DPNSS network services (UK only) 331
To program IPL....334
To set Loop avoidance during hardware configuration....335

Private networking: Using destination codes 339

Private networking: PRI Call-by-Call services 343

Configuring voice messaging 347

Configuring centralized voice mail 351
To configure the host system 353
To set up a satellite system for voice mail....354
To set up a PRI connection on the system....356

Dialing plan: Line pools and line pool codes 357

VoIP overview 363

VoIP trunk gateways 367

Configuring VoIP trunk gateways 381

VoIP interoperability: Gatekeeper configuration 389

Setting up VoIP trunks for fallback 391
To add the PSTN route to other system....392
To add the PSTN route to the local PSTN lines....392
To add the VoIP route....392
To assign PSTN line pool (to other system)....392
To assign PSTN line pool to local PSTN lines....393
To assign VoIP line pool....393
To create destination codes for your fallback route....393
To configure the VoIP schedule for all fallback destination codes....394
To set up the VoIP schedule for routing services....395
To activate the VoIP line from the control set....396
To deactivate a schedule....396

T.38 fax 401
To verify codecs in Element Manager....401
To enable a T.38 fax....402

Port ranges overview 405

Port Ranges panel 407
To add new port ranges in the RTP over UDP table....408
To delete port ranges from the RTP over UDP table....408
To modify an entry on the RTP over UDP table....409
To add new port ranges in the UDP table....409
To delete port ranges from the RTP over UDP table....409
To modify an entry on the UDP table....410

Media gateways overview 411

Media Gateways panel 413

Call security and remote access 415

Call Security: Configuring Direct Inward System Access (DISA) 427

Call security: Restriction filters 433
To add a restriction filter 435

Call security: Remote access packages 439

Configuring CoS passwords for remote access 443
To add or modify a CoS password 445
To access the system over a public network 447
To bypass the restriction filters on a telephone 447

LAN overview 449

Configuring the BCM with a DHCP address 451
To configure the BCM with a DHCP address 451

Data networking overview 453

IP Subsystem 455
To modify an IP address 456
To modify a subnet 459
To add a new IP Static Route 463
To modify an existing IP Static Route 463
To delete an existing IP Static Route 463

Data network prerequisites checklist 465

Router overview 469

Router panel 471
To access your router 471

VLAN overview 473

DHCP overview 475

DHCP Server Settings panel 481
To add a new Included Address Range 488
To delete an Included Address Range 488
To add a Reserved Address 488
To delete a Reserved Address 488

DHCP configuration with router 491
To configure the BCM with a DHCP address 491

To configure the BCM DHCP component 491
To disable the DHCP server 493

Firewall configuration resources 495

Dial Up overview 497

Dial Up Interfaces panel 501
To add an ISDN interface 503
To enable an ISDN interface 503
To disable an ISDN interface 503
To manually connect an ISDN interface 504
To disconnect an ISDN interface 504
To delete an ISDN interface 504
To modify the characteristics of an existing ISDN channel 506
To configure the ISDN Link Parameters 507
To add the modem interface 508
To enable the modem interface 509
To disable the modem interface 509
To manually connect the modem interface 509
To disconnect a modem interface 510
To delete a modem interface 510
To configure the Modem Link Parameters 511
To configure the Modem IP Address Specification 512
To assign a modem interface for WAN failover 514
To assign an ISDN interface for WAN failover 514
To add an automatic dial-out interface 522
To manually disconnect an auto dial-out interface 522

VPN overview 525

Silence suppression 529

ISDN overview 535

Codec rates 549

Index 551

Chapter 1
Getting started with BCM

Refer to the following topics for general BCM information:

- "About BCM"
- "Symbols and conventions used in this guide" on page 28
- "Related publications" on page 29
- "How to get Help" on page 31

About this guide

The *Networking Configuration Guide* describes how to configure and assign features to telephony devices through Telset and through Element Manager.

Purpose

The concepts, operations, and tasks described in this guide relate to the BCM software. This guide provides task-based information about how to assign features and provide basic programming for the BCM.

Use Element Manager, Startup Profile, and Telset Administration to configure various BCM parameters.

In brief, the information in this guide explains:

- global telephony settings
- steps to configure DNs
- product features and how to assign them

Audience

The *Networking Configuration Guide* is directed to installers who install, configure, and maintain BCM systems.

To use this guide, you must:

- be an authorized BCM installer or administrator within your organization
- know basic Nortel BCM terminology
- be knowledgeable about telephony and IP networking technology

Acronyms

The following is a list of acronyms used in this guide.

Table 1 Acronyms

Acronym	Description
ASM	Analog station module
ATA	analog terminal adapter
BRI	Basic Rate Interface
BCM	Business Communications Manager
CAP	Central Answering Position
CC	Contact Center
CLID	Calling Line Identification
CoS	Class of Service
DPNSS	Digital Private Network Signaling System
ISDN	Integrated Services Digital Network
KIM	Key Indicator Module
MCDN	Meridian Customer Defined Networking
MCID	malicious call identification
MWI	message wait indicator
OLI	outgoing line identification
ONN	outgoing name and number
PVQM	proactive voice quality monitoring
SM	silent monitor
SWCA	system-wide call appearance

Organization

This guide is organized for easy access to information that explains the concepts, operations, and procedures associated with the BCM system.

About BCM

The BCM system provides private network and telephony management capability to small and medium-sized businesses.

The BCM system:

- integrates voice and data capabilities, VoIP gateway functions, and QoS data-routing features into a single telephony system
- enables you to create and provide telephony applications for use in a business environment

BCM features

BCM50 supports the complete range of IP telephony features offered by existing BCM products:

Note: You enable the following features by entering the appropriate keycodes (no additional hardware is required).

- VoIP Gateway (H.323 and SIP): Up to 12 VoIP trunks
- VoIP Telephony Clients: Up to 32 VoIP Telephony clients, supporting the range of Nortel IP Phones and softclients.

BCM applications

BCM50 supports many applications provided on the existing BCM platforms.

Note: You enable the following features by entering the appropriate keycodes (no additional hardware is required).

- Voice Messaging for standard voice mail and auto-attendant features
- Unified Messaging providing integrated voice mail management between voice mail and common e-mail applications
- Fax Suite providing support for attached analog fax devices
- Voice Networking features
- LAN CTE (computer telephony engine)
- IP Music
- Intelligent Contact Center

Symbols and conventions used in this guide

These symbols are used to highlight critical information for the BCM system:

Caution: Alerts you to conditions where you can damage the equipment.

Danger: Alerts you to conditions where you can get an electrical shock.

Warning: Alerts you to conditions where you can cause the system to fail or work improperly.

Note: Alerts you to important information.

Tip: Alerts you to additional information that can help you perform a task.

Security Note: Indicates a point of system security where a default should be changed, or where the administrator needs to make a decision about the level of security required for the system.

Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.

Warning: Alerts you to remove the BCM main unit and expansion unit power cords from the ac outlet before performing any maintenance procedure.

The following conventions and symbols are used to represent the Business Series Terminal display and dialpad.

Convention	Example	Used for
Word in a special font (shown in the top line of the display)	Pswd:	Command line prompts on display telephones.
Underlined word in capital letters (shown in the bottom line of a two-line display telephone)	PLAY	Display option. Available on two line display telephones. Press the button directly below the option on the display to proceed.
Dialpad buttons	#	Buttons you press on the dialpad to select a particular option.

The following text conventions are used in this guide to indicate the information described:

Convention	Description
bold Courier text	Indicates command names and options and text that you must enter. Example: Use the **info** command. Example: Enter **show ip** {**alerts**|**routes**}.
italic text	Indicates book titles.
plain Courier text	Indicates command syntax and system output (for example, prompts and system messages). Example: `Set Trap Monitor Filters`
FEATURE HOLD RELEASE	Indicates that you press the button with the coordinating icon on whichever set you are using.

Related publications

This section provides a list of additional documents referred to in this guide. There are two types of publications: Technical Documents on page 29 and User Guides on page 30.

Technical Documents

System Installation

BCM50 2.0 Installation and Maintenance Guide (NN40020-302)

Keycode Installation Guide (NN40010-301)

System Programming

Administration Guide (NN40020-600)

Device Configuration Guide (NN40020-300)

Telset Administration Guide (NN40020-604)

BCM50a Integrated Router Configuration — Basics (N0115790)

BCM50a Integrated Router Configuration — Advanced (N0115791)

BCM50e Integrated Router Configuration — Basics (N0115788)

BCM50e Integrated Router Configuration — Advanced (N0115789)

Telephones and Peripherals

Telephony Device Installation Guide (NN40020-309)

Digital Mobility

T7406 Cordless Handset Installation Guide (P0606142)

IP Telephony

BCM IP Softphone 2050 Installation Guide (N0022555)

WLAN IP Telephony Installation and Configuration Guide (N0060634)

User Guides

Telephones and Peripherals

BCM Telephone Features User Guide (N0060608)

BST Doorphone User Guide (P0605668*)*

Central Answering Position (CAP) User Guide (P0603480)

Hospitality Features Card (N0027326)

System-wide Call Appearance (SWCA) Features Card (N0027186)

T7000 Telephone User Card (P0912061)

T7100 Telephone User Card (P0609621)

T7208 Telephone User Card (P0609622)

T7316 Telephone User Card (P0935248)

T7316E Telephone User Card (P0609623)

IP Phone 1120E User Guide (NN-10300-062)

IP Phone 1140E User Guide (NN-10300-064)

IP Audio Conference Phone 2033 User Guide (N0060623)

IP Key Expansion Module (KEM) User Guide

Digital Mobility

DECT 413X/414X Handset User Guide (N0028550)

DECT 4145Ex/4146Ex Handset User Guide (XXXXX)

Digital Mobility Phone 7420 User Guide (N0000635)

Digital Mobility Phone 7430/7440 User Guide (N0028550)

T7406 Cordless Telephone User Card (P0942259)

IP Telephony

IP Audio Conference Phone 2033 User Guide (N0060623)

IP Phone 2001 User Guide (N0027313)

IP Phone 2002 User Guide (N0027300)

IP Phone 2004 User Guide (N0027284)

IP Phone 2007 User Guide (N0064498)

BCM WLAN 2210/2211/2212 Handset User Guide (N0009103)

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best source of support for Nortel products is the Nortel Support Web site:

http://www.nortel.com/support

This site enables customers to:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base
- open and manage technical support cases

Getting Help over the telephone from a Nortel Solutions Center

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can get help over the telephone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the Web site below and look up the telephone number that applies in your region:

http://www.nortel.com/callus

When you speak to the telephone agent, you can reference an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, you can contact the technical support staff for that distributor or reseller.

Chapter 2
System telephony networking overview

The system supports both public and private networking for telephony traffic.

- The public network is created by PSTN trunk connections from a Central Office terminating on a telephone system such as the BCM.
- A private network is created when the system is connected through dedicated PSTN lines or VoIP trunks to other systems. This system may take several forms. At the simplest level, your system may be behind a private PBX, which connects directly to the Central Office. A more complicated system may be a node in a network of systems of various types, where calls not only terminate at the system, but calls may need to be passed through the system to other nodes unconnected to the originating node.

Refer to the following information:

- "Basic system configurations"
- "Private network parameters" on page 37

Basic system configurations

In the most basic application, your system can provide support for system telephones to make and receive calls over public network (PSTN) lines.

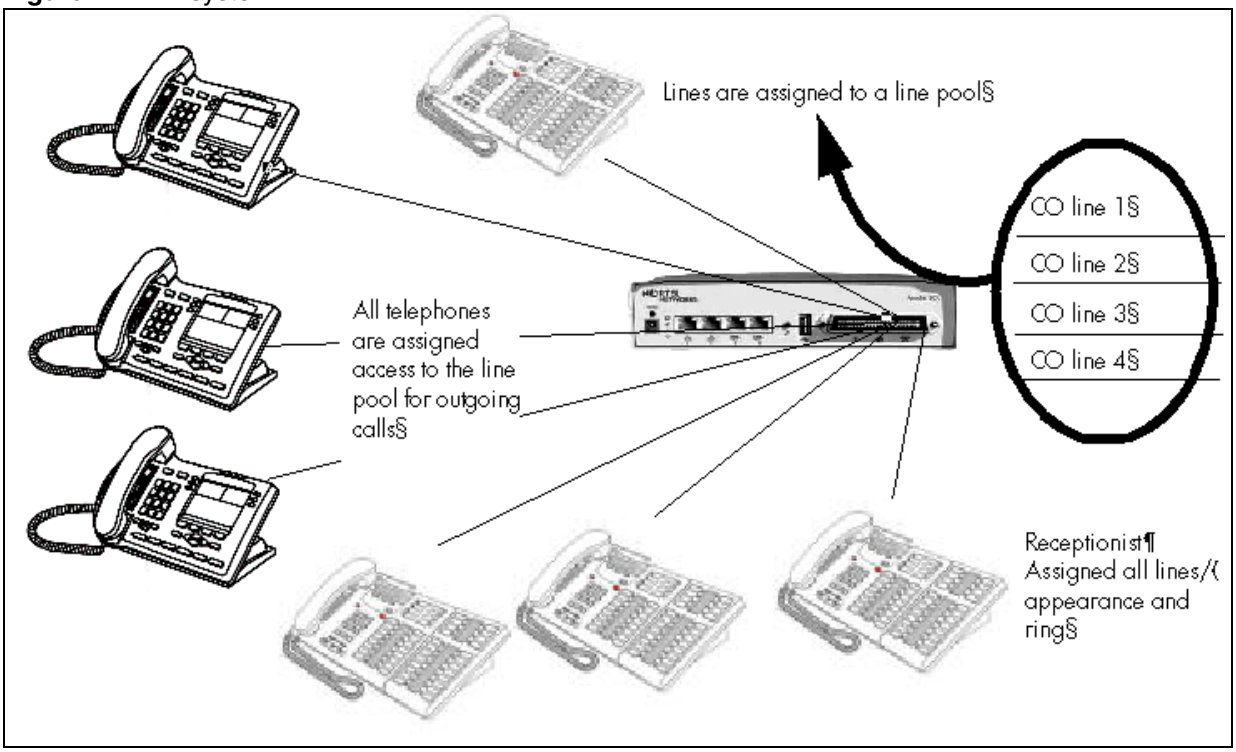
Two basic system telephony configurations

The following provides a broad overview of the telephony setup for two of the most common office-telephone configurations.

PBX system

This setup is for larger offices which have fewer CO lines than telephones. In this case the lines are pooled, and the line pool access is assigned to all DNs. There may also be a designated attendant with a telephone that has all lines individually assigned.

Figure 1 PBX system



Incoming calls

1. A call comes in on a line.
2. The receptionist answers the call and finds out who the call is for.
3. The receptionist transfers the call to a specific telephone (DN).
4. The person can pick up the call at that DN only.

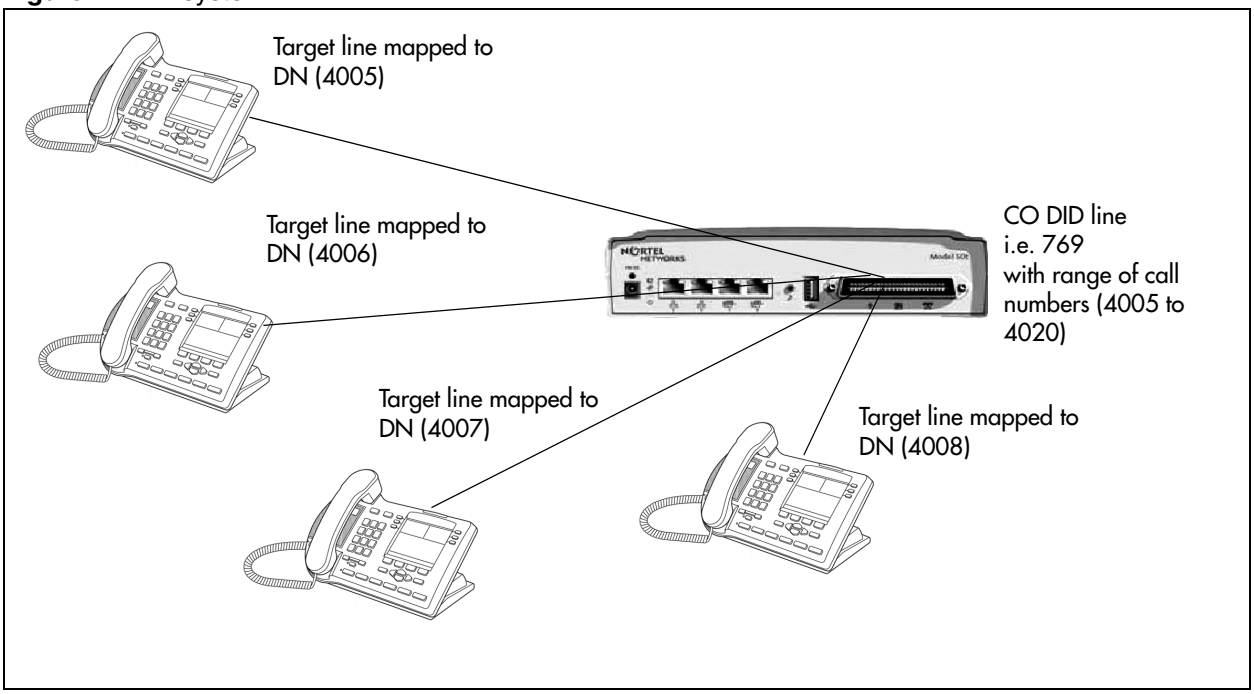
Outgoing calls

1. User selects the intercom button or dials a line pool access code, which selects a line in the line pool.
2. The user dials the outgoing telephone number.

DID system

This setup allows you to assign a dedicated phone number to each telephone. The CO assigns a list of available numbers for each DID (Direct Inward Dial) line. You can change your DN range to match these numbers, and you use target lines to match each number with a DN.

Figure 2 DID system



Incoming calls

1 DID trunks are assigned to be auto-answer.

Note: PRI lines are automatically set to auto-answer.

2 All DNs are assigned target lines.

3 A caller dials a system code and a DN. In the example shown above, it might be 769-4006.

4 The call comes into the trunk, which answers and maps the call on the target line assigned to the matching received digits.

5 The DN assigned to that target line rings.

You can assign unanswered or busy telephones to Call Forward to another DN, such as a designated attendant or a voice-mail system.

Basic telephony routing

In a basic configuration, simple access codes (for example Line Pool Codes) are used to access the PSTN network.

In a more complex configuration, more advanced destination codes are required to access multiple PSTNs, private network resources, and remote nodes. Access to these resources enables advanced features, such as tandem routing.

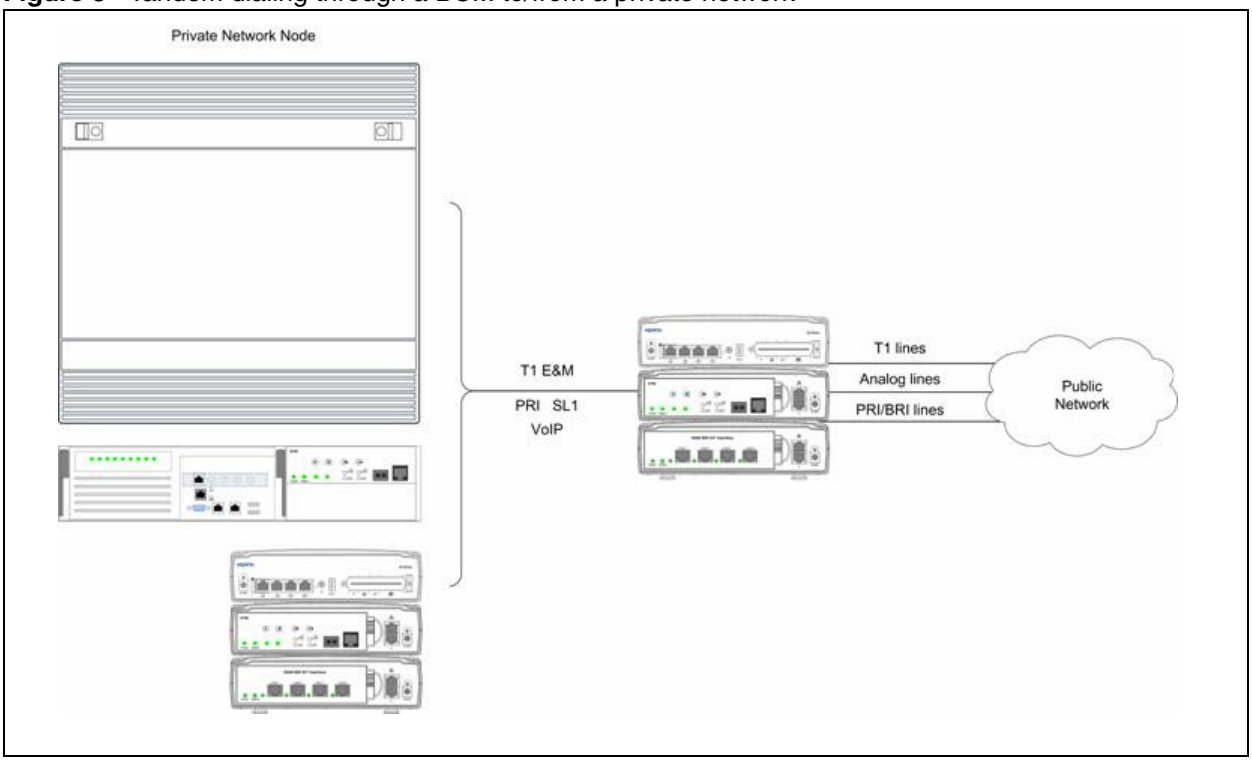
Tandem calling to a remote PSTN

A system connected to a private network that uses dedicated circuits or VoIP circuits can allow a user to dial directly to many other users, on different nodes, using a coordinating dialing plan.

Using a private network saves on toll charges, and local charges, as fewer PSTN accesses are required for internal and external calling. Several nodes located on one site initiate their external local calls to a centralized BCM having a T1 termination to the PSTN. This type of configuration avoids multiple PSTN terminations at other local nodes.

The same tandeming concepts can be applied to inbound calls. DID numbers dialed from the PSTN can be processed and tandem routed out of the centralized system to the localized remote nodes. See other details on Tandem routing “Creating tandem private networks” on page 43.

Figure 3 Tandem dialing through a BCM to/from a private network



In the above example, there are three types of callers.

Each type of caller has a specific method of accessing the other two systems.

Callers using BCM

These callers can:

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network

- select an outgoing central office line to access the public network
- use all of the BCM features

Callers in the public network

These callers use the public lines to:

- call directly to one or more BCM DNs
- call into BCM and select an outgoing TIE line to access a private network
- call into BCM and select an outgoing central office line to access the public network
- call into BCM and use remote features

Callers in the private network node

These callers use the private lines to:

- call directly to one or more BCM DNs
- call into BCM and select an outgoing TIE line to access other nodes in a private network
- call into BCM and select an outgoing central office line to access the public network
- call into BCM and use remote features

System numbering and dialing plans

All systems on a private network must coordinate dialing plans, to ensure that calls get directed to the correct network node. As well, routing becomes more complex, especially if the system is not an end node and must be configured to relay calls to nodes not directly connected to the system. The type of dialing plan supported by the network determines whether each node also requires unique DNs.

Private network parameters

The following provides an overview of the system values that affect private networking.

Private networking protocols

The BCM supports the following protocols for private networking:

- PRI: ETSI QSIG, Nortel Voice Networking (MCDN)

- DPNSS
- BRI: ETSI QSIG
- T1: E&M
- VoIP trunks (with optional MDCN)

Note: MCDN is referred to as SL-1 in Element Manager.

BCM systems can be networked together using T-1, PRI or VoIP trunks. PRI SL-1 lines and VoIP trunks also offer the opportunity to use the MCDN protocol, which provides enhanced trunking features and end-to-end user identification. If a Meridian 1 is part of the MCDN network, the network can also provide centralized voice mail and auto attendant off the Meridian.

MCDN note: MCDN networking requires all nodes on the network to use a common Universal Dialing Plan (UDP) or a Coordinated Dialing Plan (CDP).

Keycode requirements

Keycodes are required to activate the protocols that are used to create private networking, including:

- VoIP Gateway keycodes
- an MCDN, DPNSS, or Q. Sig keycode, if you want to use a networking protocol between the systems

You must purchase and install these keycode*s* before you can create any of the networks described in this chapter. Consult with your Nortel distributor to ensure you order the correct keycodes for the type of network you want to create.

Remote access to the network

Authorized users can access TIE lines, central office lines, and features from outside the system. Remote users accessing a private network configured over a large geographical area can avoid toll charges.

Note: You cannot program a DISA DN or Auto DN to a VoIP trunk, as they act as auto-answer trunks from one private network to the next. However, you can configure VoIP line pools with remote access packages so that callers can access telephones or the local PSTN on remote nodes on a tandemed network that use VoIP trunks between systems.

Lines used for networking

External (trunk) lines provide the physical connection between BCM and other systems in a private or public network.

The BCM50 numbers physical lines from 061 to 124. Default numbering depends on the type and connection to the BCM (EXP1 - EXP2).

VoIP trunks: Although a VoIP gateway does not use physical lines, it is easier to think of them that way. Therefore, in the BCM, lines 001 to 012 are used for VoIP trunk functionality.

BCM networking configurations that use PRI and T1 lines, require specific DTM modules.

- DTMs configured for PRI are used for incoming and outgoing calls (two-way DID). Incoming calls are routed directly to a BCM DN that has a properly configured and assigned target line. All outgoing calls made through PRI, are initiated using the destination codes.
- DTMs configured for T1 can have digital lines configured as Groundstart, E&M, Loop, or DID.

Target lines are virtual communication paths between trunks and telephones on the BCM system. They are incoming lines only, and cannot be selected for outgoing calls or networking applications. With target line*s*, you can concentrate incoming calls on fewer trunks. This type of concentration is an advantage of DID lines. BCM target lines allow you to direct each DID number to one or more telephones. VoIP trunks also require target lines to direct incoming traffic. Target lines are numbered 125 to 268.

Telephones can be configured to have an appearance of analog lines or multiple appearances of target lines.

Note: PRI B-channels cannot be assigned as line appearances. PRI B-channels, or “trunks”, can only be configured into PRI line pools for inbound routing through target lines with receive digits or outbound routing through destination codes.

Types of private networks

There are several ways you can create private networks. Configuration can be based on such things as cost of trunks, proximity of network nodes, size of the private network, and business requirements for communications.

VoIP-based networking also requires an understanding of IP features such as codecs, jitter buffers, Quality of Service (QoS) function, and silence compression.

The services provided within networks is based on the type of trunks and the protocols assigned to the trunks. All trunks within the network should be running the same protocols, to provide a technically sound and stable network.

The following links are procedures to set up basic networks to advanced networks, using the support protocols within BCM:

- “Routing-based networks using T1 E&M lines” on page 40

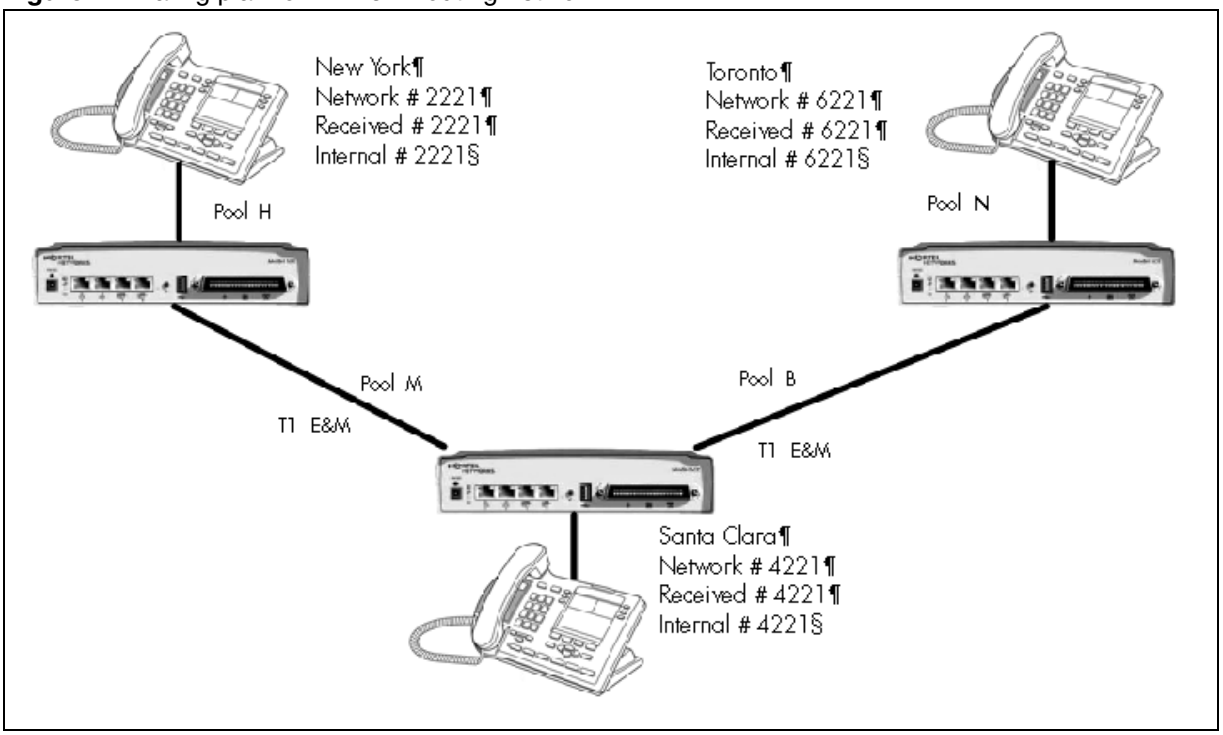
- "PRI networking using Call-by-Call services" on page 41
- "PRI SL-1/Q.Sig/DPNSS and VoIP trunk networking" on page 42

Routing-based networks using T1 E&M lines

By properly planning and programming routing tables and destination codes, an installer can create a dialing plan where T1 E&M lines between BCM systems are available to other systems in the network

Figure 4 shows a network of three BCM systems. Two remote systems connect to a central system.

Figure 4 Dialing plan for T1 E&M routing network



Each system must be running BCM software. Each system must be equipped with target lines and a BCM expansion unit with a DTM with at least one T1 E&M line.

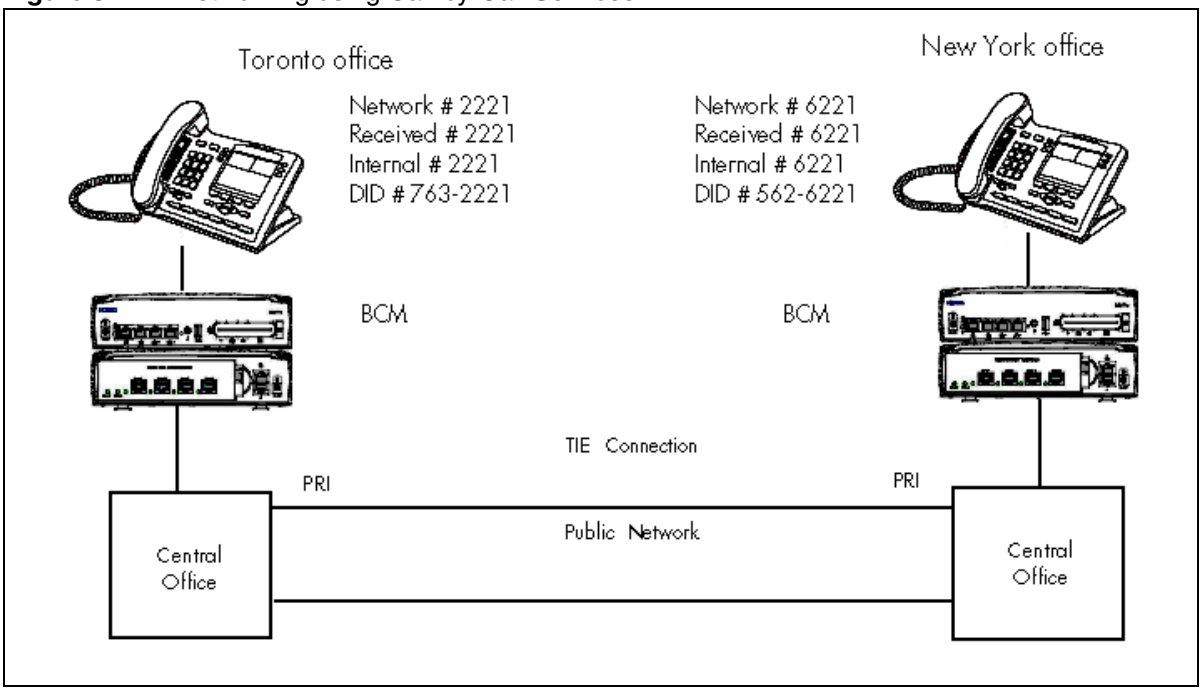
The call appears on the auto answer line on the BCM in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 002 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line Private received number. The call now alerts at DN 6221 in Toronto.

Note: Network calls that use routes are subject to any restriction filters in effect. If the telephone used to make a network call has an appearance of a line used by the route, the call will move from the intercom button to the Line button. The telephone used to make a network call must have access to the line pool used by the route. Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal telephone numbers. Routes generally define the path between your BCM switch and another switch in your network, not other individual telephones on that switch.

PRI networking using Call-by-Call services

The example shown in Figure 5 highlights the use of PRI Call-by-Call services. It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with a BCM system and a PRI line. Each office has to handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office. Refer to “Private networking: PRI Call-by-Call services” on page 343 for more information.

Figure 5 PRI networking using Call-by-Call Services



To reduce long distance costs, and to allow for a coordinated dialing plan between the offices, private lines are used to handle inter-office traffic.

If call-by-call services were *not* used, each BCM system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic.
- eight T1 E&M lines needed to handle inter-office calls.
- eight lines needed to handle outgoing public calls

PRI SL-1/Q.Sig/DPNSS and VoIP trunk networking

You can use PRI SL-1 trunks and VoIP trunks to create private networks between BCM systems or between BCM systems and larger call servers such as Meridian 1, Succession 1000/M, DMS-100/250 and CSE.

ETSI-QSIG and DPNSS private networking is configured very similarly, although network features may be supported slightly differently due to local line and network requirements.

If the MCDN protocol is added to this type of private network, the network provides additional network management features, as well as allowing centralized voice mail features to be available to all nodes on the network.

The following topics describe the different aspects of SL-1 and MCDN private networking.

- “System dialing plans” on page 43
- “Creating tandem private networks” on page 43

- "Understanding Nortel Voice Networking (MCDN) network features" on page 46
- "Networking with ETSI QSIG" on page 50
- "Private networking with DPNSS" on page 60

The type of network you require depends on the equipment in the network, and how you want to use the network.

- With MCDN, you can tie a set of BCM systems together with PRI SL-1 (MCDN)/ETSI-QSIG, DPNSS, or VoIP trunks to create a tandem network. This type of network provides the additional advantage of providing private line access to local PSTNs for all the nodes on the network.

Note: A keycode is required to use the Nortel Voice Networking functionality which is referred to as SL-1 in the BCM Element Manager.

System dialing plans

Both of these types of networks require similar setups for dialing plans and routing. Each node must have a way to route external calls to the adjacent node or nodes. To do this, all nodes must have the same Private DN lengths.

You use routing and a private dialing plan to control calls over the network. Each example in this section describes the routing configurations that are required to support calls over the network.

Depending on the type of dialing plan you choose, each node must also have a unique location or steering code so the calls can be correctly routed through the nodes of the network. MCDN networks also require a Private Network ID, which is supplied by the Meridian network administrator to define how the Meridian system identifies each node.

Creating tandem private networks

You can tie a number of BCM systems together with SL-1 lines. This tandem network provides you with the benefits of end-to-end name display and toll-free calling over the SL-1 private link. Each BCM system becomes a node in the network. In this type of network, you must ensure that each BCM system, known as a node of the network, is set up to route calls internally as well as to other nodes on the system. This means each node must have a route to the immediately adjacent node, and the correct codes to distribute the called numbers. Each node must have a unique identification number, which is determined by the type of dialing plan chosen for the network.

As well, you can save costs by having a public network connection to only one or two nodes, and routing external calls from other nodes out through the local PSTN, thus avoiding toll charges for single calls.

VoIP note: You can also use VoIP trunks between some or all of the nodes. The setup is the same, except that you need to create gateway records for each end of the trunk, and routing tables to accommodate the gateway codes, or you can configure a gatekeeper. Refer to "VoIP interoperability: Gatekeeper configuration" on page 389.

Routing for tandem networks

In tandem networks, each node needs to know how to route calls that do not terminate locally. To do this, you set up routes for each connecting node by defining destination codes for each route.

If the node is also connected to the public network, the usual routing is required for that connection.

The following tables show the routing tables for Node A and Node C for external and internal terminating calls.

Note: The PRI and VoIP trunks are en bloc dialing lines, so all dialed digits are collected before being dialed out.

Table 1 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	91604
3 (Node B)	0	91403762 (Node B)
3 (Node B)	0	91403765 (Node E)
4 (PSTN)	1	9140376* (not internal network)
4 (PSTN)	1	914037* (not internal network)
4 (PSTN)	1	91403* (not internal network)
4 (PSTN)	1	9* (not internal network)
* This wild card represents a single digit.		

Table 2 Node A destination code table, internal termination

Route	Absorb length	Destination code (private DNs)
3 (Node B)	0	392 (Node B)
3 (Node B)	0	395 (Node E)
5 (Node C)	0	393 (Node C)
5 (Node C)	0	394 (Node D)
5 (Node C)	0	396 (Node F)

Table 3 Node C destination code table, external termination

Route	Absorb length	Destination code (Public DNs)
3 (Node B)	0	91613764 (Node D)
3 (Node B)	0	91613766 (Node F)
4 (PSTN)	1	9161376* (not internal network)
4 (PSTN)	1	916137* (not internal network)
4 (PSTN)	1	91613* (not internal network)
4 (PSTN)	1	9161* (not internal network)
4 (PSTN)	1	916* (not internal network)
4 (PSTN)	1	91* (not internal network)
4 (PSTN)	1	9 (not internal network)
* This wild card represents a single digit.		

Table 4 Node C destination code table, internal termination

Route	Absorb length	Destination code (Private DNs)
3 (Node D)	0	394 (Node D)
3 (Node D)	0	396 (Node F)
5 (Node A)	0	391 (Node A)
5 (Node A)	0	392 (Node B)
5 (Node A)	0	395 (Node E)

Understanding Nortel Voice Networking (MCDN) network features

When you connect your BCM systems through PRI-SL-1/ETSI QSIG/DPNSS or VoIP trunks, and activate the MCDN protocol, your network provides a number of network call features. You can use this protocol to network other BCM systems, such as the tandem system shown in "Creating tandem private networks", Norstar systems, Meridian 1 systems, Succession systems, DMS-100 systems or CSE systems.

Table 5 lists the MCDN features that are provided by all SL-1/VoIP networks where MCDN is active. The features affect call redirection and trunking functions.

Table 5 MCDN network features

Centralized messaging	"Network Call Redirection Information" on page 46 (NCRI)
Centralize trunking	"ISDN Call Connection Limitation" on page 47 (ICCL) "Trunk Route Optimization" on page 48 (TRO) "Trunk Anti-tromboning" on page 49 (TAT)

Network Call Redirection Information

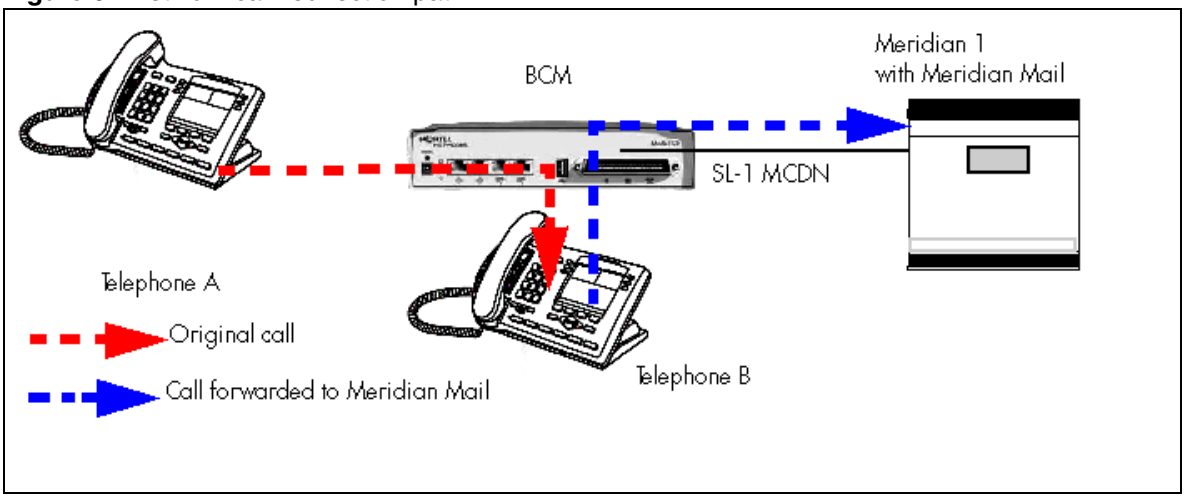
Network Call Redirection Information (NCRI) builds on the following BCM features:

- External Call Forward
- Call Transfer
- Call Forward

NCRI adds the ability to redirect a call across an MCDN network using Call Forward (All Calls, No Answer, Busy) and Call Transfer features. The call destination also receives the necessary redirection information. This feature allows the system to automatically redirect calls from within a BCM system to the mail system, such as Meridian Mail, which resides outside the BCM system on the Meridian 1.

Figure 6 shows an example of this situation, where user A calls user B on the same BCM. If user B is busy or not answering, the call automatically gets transferred to a Meridian Mail number (user C) across an MCDN link between the BCM system and the Meridian 1 system where the mailboxes are set up.

Figure 6 Network call redirection path



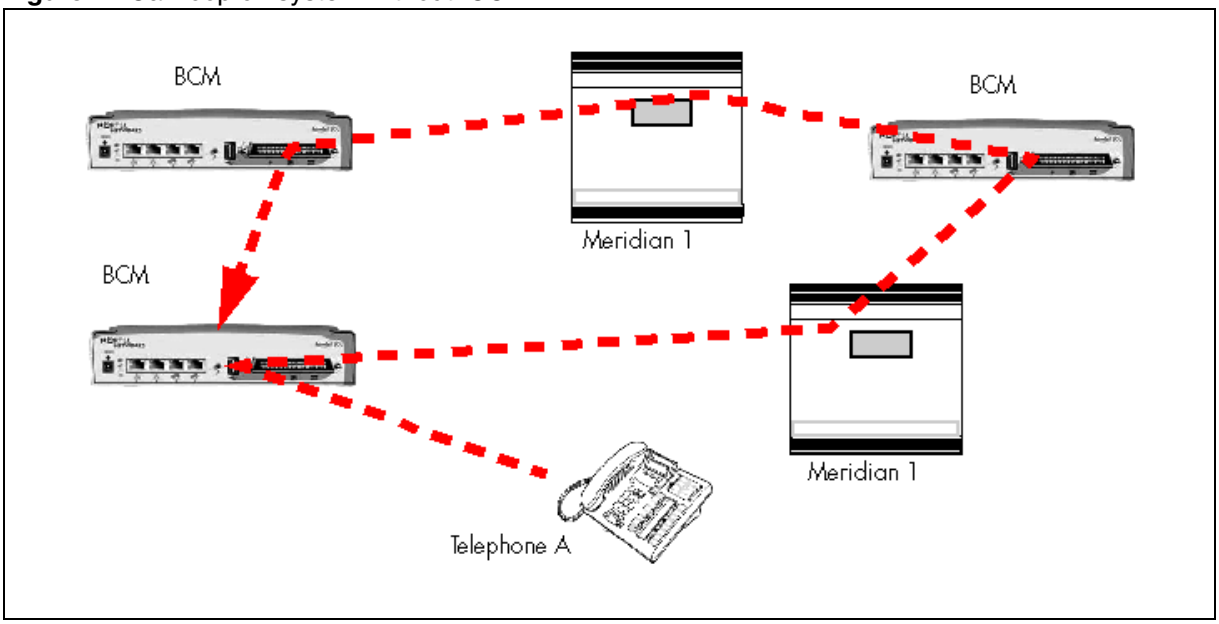
ISDN Call Connection Limitation

The ICCL (ISDN Call Connection Limitation) feature piggybacks on the call initiation request and acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels. Also refer to "ISDN overview" on page 535.

This feature adds a transit/tandem counter to a call setup message. This counter is compared at each transit PBX with a value programmed into the transit PBX, in a range from 0 to 31. If the call setup counter is higher than the PBX value, the call will be blocked at the PBX system and cleared back to the network. This prevents calls from creating loops that tie up lines.

Figure 7 demonstrates how a call might loop through a network if the system is not set up with ICCL.

Figure 7 Call loop on system without ICCL



Trunk Route Optimization

Trunk Route Optimization (TRO) finds the most direct route through the network to send a call between nodes. This function occurs during the initial alerting phase of a call.

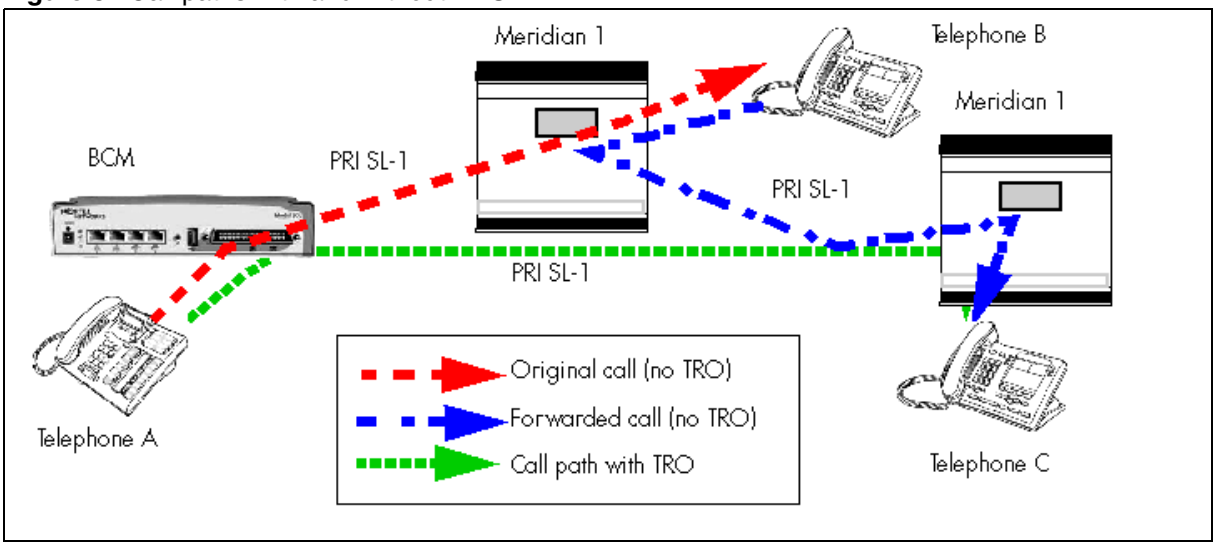
To set BCM configurations:

- Select **Configuration > Dialing Plan > Private Network**, and select the check box beside TRO.
- Configure call routing for all optimal routes.
- Configure call forward (All Calls, No Answer, Busy) or Selective Line Redirection to use the optimal routes.

This feature avoids the following situation: A call originating from a BCM system may be networked to a Meridian system, which, in turn, is networked to another Meridian system, which is the destination for the call. If the call routes through the first Meridian (M1) to reach the second Meridian (M2), two trunks are required for the call. An optimal choice is a straight connection to M2. This finds these connections and overrides the less-efficient setup.

Figure 8 shows two call paths. The first route, through the Meridian, demonstrates how a call might route if TRO is not active. The second route, that bypasses the Meridian, demonstrates how TRO selects the optimum routing for a call.

Figure 8 Call paths with and without TRO



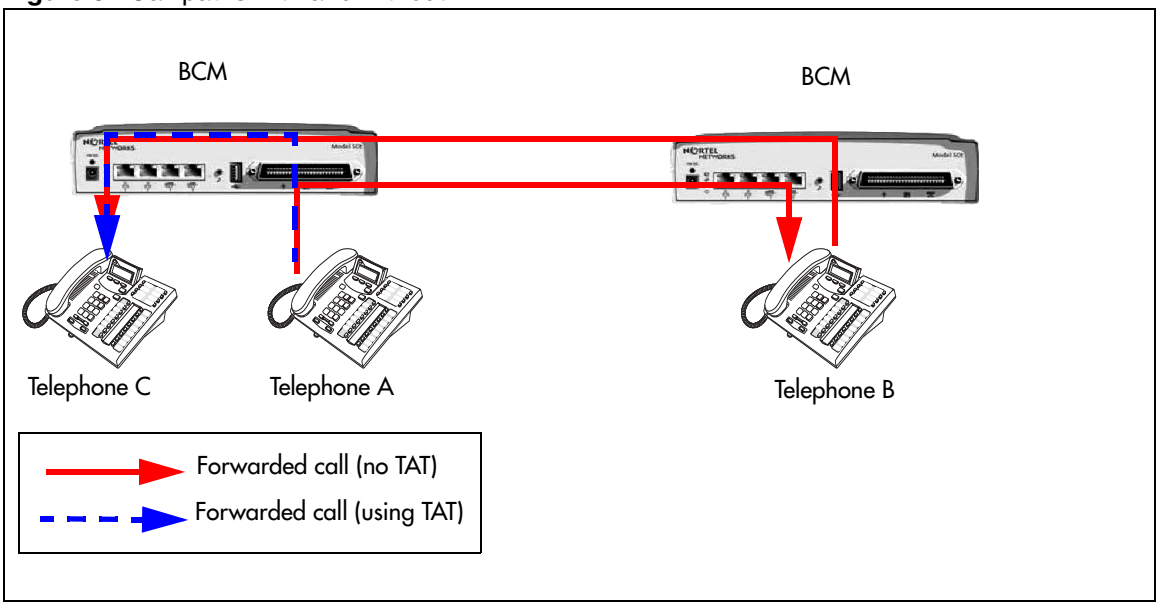
Trunk Anti-tromboning

Trunk Anti-Tromboning (TAT) is a call-reroute feature that works to find better routes during a transfer of an active call. This feature acts to prevent unnecessary tandeming and tromboning of trunks.

Note: This feature is not applicable for alerting calls.

Figure 9 shows how TAT reduces the line requirements. The solid line shows Telephone A calling Telephone B and being transferred over an additional PRI line to Telephone C. With TAT active, the same call is transferred to Telephone C over the same PRI line.

Figure 9 Call paths with and without TAT



Networking with ETSI QSIG

(International systems only)

ETSI QSIG is the European standard signaling protocol for multi-vendor peer-to-peer communications between PBX system*s* and/or central offices.

See: "ETSI Euro network services" on page 51.

Figure 10 illustrates an ETSI QSIG network. Note that this is exactly the same setup as that shown in the MCDN section for North America. The hardware programming for ETSI QSIG is described in Table 6. All other configurations are the same as those shown in the MCDN section for North America.

Figure 10 ETSI QSIG networking

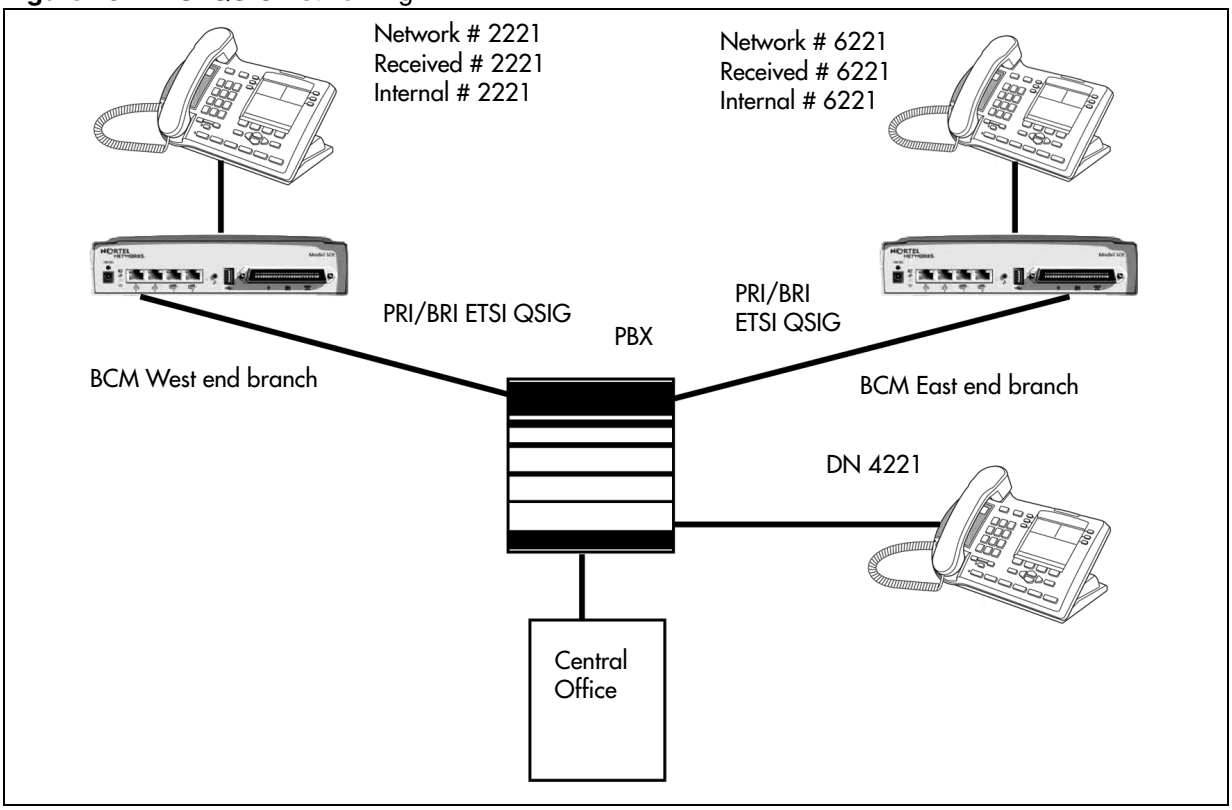


Table 6 lists the settings for some of the hardware parameters for ETSI QSIG networking example shown in Figure 10.

Table 6 Hardware programming for branch offices

West End office:		
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

East End office:		
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

ETSI Euro network services

If your system has ETSI ISDN BRI/PRI lines, you can activate the malicious call identification (MCID) and Network Diversion features. Advice of charge-end call (AOCE) is active if your service provider has activated that service on the line.

When the features are activated, users can:

- display a call charge
- redirect calls over the ETSI ISDN BRI/PRI line to the outside network
- tag malicious calls

Advice of Charge-End of Call (AOCE) — AOCE is a supplementary service available from your service provider on ETSI ISDN BRI/PRI links. This feature allows the BCM user to view the charges for an outgoing call after the call completes. This information is also reported to the Call Detail Reporting Application. The information can be provided in currency or charging units, depending on how the feature is set up by your service provider.

To invoke the feature, the user presses **FEATURE 818**.

DPNSS 1 services

The Digital Private Network Signaling System (DPNSS 1) is a networking protocol enhancement that extends the private networking capabilities of existing BCM systems. It is designed to offer greater centralized functionality for operators, giving them access to BCM features over multiple combined networks.

Note: The DPNSS feature is dependent on which region loaded on your system at startup and that a software keycode was entered to enable the feature.

For more information, see:

- “DPNSS 1 capabilities” on page 53
- “DPNSS 1 features” on page 53
- “Private networking with DPNSS” on page 60

DPNSS 1 allows a BCM local node, acting as a terminating node, to communicate with other PBXs over the network. For example, corporate offices separated geographically can be linked over DPNSS 1 to other BCM nodes, bypassing the restrictions of the PSTNs to which they may be connected. Connected BCM nodes can therefore function like a private network, with all features of BCM accessible.

Note: BCM DPNSS 1 works as a terminating node only. BCM-to-BCM DPNSS is not supported.

You can use DPNSS 1 features on any BCM telephone. On most BCM telephones, you must use specific keys and/or enter a number code to access the features.

DPNSS 1 capabilities

A single BCM node, acting as a terminating node on the network, supports the following capabilities over DPNSS 1 lines:

- Direct Dial Inward (DDI) for incoming calls.
- Originating Line Identification (OLI) for incoming and outgoing calls:
  - For incoming calls, the Calling Line Identification (CLI/CLID) information is displayed to the user on telephones with line display. This must be configured in programming.
  - For outgoing calls, the directory number of the originating party is sent out as OLI.
- Terminal Line Identification (TLI) for incoming and outgoing calls. Referred to as Called Line Identification.
- Selective Line Redirect (SLR) and External Call Forward (ECF) implemented on calls between DPNSS 1, and BRI/PRI, DASS2, and analog lines.
- These remote access features are supported on DPNSS: DDI, line pool access code, destination codes and remote page feature codes.

Keycodes are required to enable DPNSS 1.

DPNSS to Embark connections

DPNSS lines connected to an Embark switch perform call redirection/diversion using the Call Forward feature to create a tandem link back to the switch. Since this is different from other switches, you must select the type of switch DPNSS will be connecting to when you do module programming.

Before you program Call Forwarding, ensure that:

- Both real channels and virtual channels are provisioned.
- Destination or line pool codes are programmed for the DPNSS to Embark link.

Also, during programming for Call Forward No Answer and Call Forward on Busy, when you enter the **Forward to:** digits, the system does a validation check with the switch on the number. (**Configuration > Telephony > Sets > Active Sets > Line Access**)

DPNSS 1 features

The following features are available and can be programmed over DPNSS lines:

- “Three party service” on page 54
- Diversion (“Using the diversion feature” on page 55)
- Redirection (“Using the Redirection feature” on page 56)
- “Executive intrusion” on page 57

- “Call Offer” on page 58
- “Route Optimization” on page 59
- “Loop avoidance” on page 59
- Message Waiting Indication

The following parameters can be configured for DPNNS 1 lines:

- Line type
- Prime set
- CLID set
- Auto privacy
- Answer mode
- Auxiliary ringer
- Full autohold

Some features are transparent to the user, but must be programmed to be activated. Others are available for end-user programming at the telephone. Details about these features are given below.

Three party service

Three Party Service is a DPNSS 1 feature for BCM that is similar to the BCM Conference feature.

The Three Party Service allows a user, usually an operator, to establish a three-party conference by calling two other parties from one telephone. Once the connection is made, the controlling party can hang up, leaving the other two connected. The controlling party can even put one party on hold, and talk to the other party.

Note: BCM does not support Hold over the DPNSS link itself. This means that the conferenced party on the distant end of the network cannot place a Three Party Service call on Hold.

This feature is designed to allow operators to assist in the connection of calls from one main location.

Making a conference call

To initiate or disconnect from a conference call on a BCM system over DPNSS 1, use the procedure described in the *Device Configuration Guide* (NN40020-300).

Note: Three Party Service is supported on model 7000 telephones, but in a receive-only fashion. These telephone types cannot initiate Three Party Service. For more information about these telephone types, see the *Telephony Device Installation Guide* (NN40020-309) (model 7000 phones, supported in Europe only).

Using the diversion feature

Diversion is a DPNSS 1 feature for BCM that allows users to forward their calls to a third party on the DPNSS 1 network. This feature is similar to Call Forward on BCM but takes advantage of the broader capabilities of DPNSS.

There are five variations of Diversion: Call Diversion Immediate, Call Diversion On Busy, Call Diversion On No Reply, Bypass Call Diversion, and Follow-me Diversion. These variations are described below:

- Diversion Immediate diverts all calls to an alternate telephone. This function is programmed by the user at their telephone.
- Diversion On Busy diverts all calls to an alternate telephone when a telephone is busy. This feature is programmed in the Element Manager.
- Diversion On No Reply diverts calls that go unanswered after a specified amount of time. This feature is programmed in the Element Manager.
- Bypass Call Diversion overrides all call forward features active on a telephone over a DPNSS line. An incoming call to the telephone will not be forwarded; instead, the telephone will continue to ring as if call forward were not active. This feature is used to force a call to be answered at that location. Bypass Call Diversion is a receive-only feature on BCM and cannot be used from a BCM telephone.
- Follow-me Diversion is also a receive-only feature. It allows the call-forwarded destination to remotely change the BCM call-forwarding programming (Call Forward All Calls [CFAC] feature) to a different telephone.

Note: BCM CFAC must be active, and the destination set/PBX system must support the feature.

For example, user A forwards all calls to telephone B, a temporary office. Later, user A moves on to location C. The user does not have to be at telephone A to forward calls to location C. Using telephone B and Follow-me Diversion, the user can forward calls from A to location C.

Follow-me diversion can be cancelled from the forwarded location.

- Diversion on Busy and Diversion on No Reply cannot be cancelled from the forwarded telephone. These are programmable only by an installer and not by the user.
- If multiple telephones are programmed to take a call, the first telephone to respond will act. All other telephones responding are ignored. Therefore, if the first telephone to respond has Diversion enabled, this feature will be invoked.

Restrictions by telephone type

- all variations supported on BCM digital and IP telephones
- ATA2/ASM8+—all variations supported on an ATA
- ISDN—all variations supported on ISDN telephones, except Diversion on Busy and CFWD Busy

Setting Diversion

You set Diversion for DPNSS in the same way as Call Forward. You will need to enter the end DN when prompted. You may also need to include the DPNSS 1 routing number.

Using the Redirection feature

Redirection is a DPNSS 1 feature similar to BCM Transfer Callback. With Redirection, a call awaiting connection, or reconnection, is redirected by the originating party to an alternate destination after a time-out period. Failed calls can also be redirected. Priority calls are not redirected.

Note: The address to redirect depends on the history of the call. Calls that have been transferred are redirected to the party that transferred them. In all other cases, the address to redirect is the one registered at the PBX system originating the redirection.

Note: BCM does not support the redirection of BCM-originated calls, even over DPNSS 1.

The Diversion on No Reply feature takes precedence over Redirection.

Restrictions by telephone type

- For telephones with a single line display, the number key (**#**) acts as MORE and the star key (*****) acts as VIEW
- ISDN—all variations supported on ISDN telephones

Setting redirection

The timer used for the network Callback feature is also used for redirection.

Executive intrusion

Executive Intrusion (EI) is a DPNSS 1 feature that allows an operator, or other calling party, to intrude on a line when it is busy. An example of the use of this feature is to make an important announcement when the recipient is on another call.

EI is similar in functionality to BCM Priority Call, but it is a receive-only feature on BCM telephones. EI cannot be initiated from a BCM telephone. The person using this feature must be on another PBX system on the DPNSS 1 network.

When EI is used to intrude on a call in progress, a three-way connection is established between the originating party and the two parties on the call. The result is very much like a conference call. When one of the three parties clears the line, the other two remain connected, and EI is terminated.

Restrictions by telephone type

- ATA2/ASM8+—supported
- ISDN—not supported

The telephone receiving the intrusion displays `Intrusion Call`. A warning indication tone will sound after intrusion has taken place, and the standard conference call tone will sound every 20 seconds.

Intrusion levels

Whether a telephone accepts or rejects an Executive Intrusion request depends on the level of intrusion protection programmed. Each telephone (DN) has an Intrusion Capability Level (ICL) and four Intrusion Protection Levels (IPL).

When the ICL of the intruding telephone is higher than the IPLs of *both* telephones on the active call, EI occurs. Nortel recommends that you set the IPLs of most BCM telephones to the default of None, or Low or Medium.

Intrusion levels are described as follows:

- ICL: determines the ability of the attendant to intrude. As long as the ICL is higher than the IPL of the wanted party, EI is allowed. Because EI is a receive-only feature, the ICL cannot be set on BCM.
- IPL: determines the ability of the attendant to refuse intrusion. If the IPL is lower than the ICL of the originating party, EI is allowed. For general purposes setting the IPL to None, Low or Medium is recommended, unless intrusion is not wanted.

Call Offer

Call Offer over DPNSS 1 allows a calling party to indicate to the wanted party that there is an incoming call available, even though there is no answer button available to present the call on the telephone. The intended recipient can ignore, accept, or decline the offered call. Call Offer is useful in increasing the call-coverage capability of a BCM system, and helps to lift the network processing load. It is a receive-only capability on BCM; incoming calls are initiated at another PBX system on the DPNSS 1 network.

An example of Call Offer in use is an operator or attendant who has a number of calls coming in at once. The operator can call offer one call and move to the next without waiting for the first call to be answered.

Call Offer Displays

When a Call Offer is made by the originating exchange, the target telephone displays a message, and a tone is heard. When an offered call arrives on telephones with line display, the user sees `XX...X wtng` if the calling party ID is available and CLID is enabled. If CLID is not available or CLID is disabled, `Line XXX waiting` appears (the line name associated with the call). If there are more than 11 digits in the incoming number, only the last 10 will display.

If Call Queuing is programmed for the system, the display shows `Release Line XXX`.

This is the line name of the highest-priority queued call if it is an offered call.

Restrictions by telephone type

- model 7000 telephone — associated LED or LCD flashes, and a tone is heard (model 7000 phones, supported in Europe only.)
- ATA2/ASM8+—Call Offer is supported as a Camp On feature, and a tone is heard
- ISDN—not supported

Note the following general conditions and restrictions:

- Clear the **DND on busy** check box (**DN ##/Capabilities**) for a telephone to accept Call Offer.
- If CF on busy is programmed for the telephone, Call Offer is not accepted.
- The target line for the telephone must be set to: If **busy: busy tone**, which is the default.
- Call Offer does not work if sent over Manual answer lines. It is recommended that the lines be left at the default: **Auto**.

User actions

The party receiving a Call Offer has three choices:

- Ignore it. After a programmed time interval, the Offer request is removed.

- Reject it. If the user activates Do Not Disturb on Busy (DND) when the Call Offer request is made, the request is removed from the telephone. The calling party is informed of the rejection.

Note: A call cannot be offered to a telephone with DND active. The line indicator for external incoming calls still flashes.

- Accept it. The Offer is accepted by releasing the active call.

Note: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

Route Optimization

Route Optimization is a DPNSS 1 feature for BCM that allows calls to follow the optimum route between two end PBXs. This allows efficient use of network resources.

Route Optimization is initiated by the system and is transparent to the user. However, the user may see a call switch from an appearance on the telephone to another appearance key or from an intercom button to the appearance key or vice versa. This occurs when BCM receives a Route Optimization request and initiates a new call to follow the optimal route.

If a telephone is active on a private line call, the Route Optimization call being established may go on a public line. This will cause a loss of privacy on that line.

Data calls are rejected by Route Optimization in order to ensure the data transmission is not affected.

Certain situations result in Route Optimization not taking place. For example, calls that are using Hold, Parking or Camp features do not undergo Route Optimization, and if a Route Optimization call undergoes Diversion, the Route Optimization is dropped.

Setting Route Optimization

System programming is not required for the feature when BCM is working as a terminating PBX system. However, BCM must have a private access code programmed that maps to a valid destination code or line pool code on DPNSS lines. Further, **Allow Redirect** must be selected.

Loop avoidance

Errors in the configuration of a network may make it possible for a call to be misrouted, and arrive at a PBX system through which it has already passed. This would continue, causing a loop which would eventually use up all of the available channels. The Loop Avoidance service permits counting of DPNSS 1 transit PBXs and rejecting a call when the count exceeds a predetermined limit.

Private networking with DPNSS

(International only)

DPNSS supports the Universal Dialing Plan (UDP), an international standard for sending and receiving private numbers over networks. The UDP requires that a dialing number include the following:

- a Private Access Code, programmed into the system as part of the destination code table to prevent conflicts with the internal numbering system. (**Access Codes**)
- a Home Location Code (HLC) assigned to each PBX system, and configured as part of the destination code (a maximum of seven digits). For each HLC, a destination code must be programmed in the system. (**Configuration > Telephony > Dialing Plan > Private Networking**)
- a Directory Number (DN) assigned to each extension as a line appearance. The DN appears as the last string segment in a dialed number. In the number 244-1111, 1111 is the DN.

A typical Private Number, using a private access code and dialed from another site on the network, appears below.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+ 848	+ 2222	= 6-848-2222

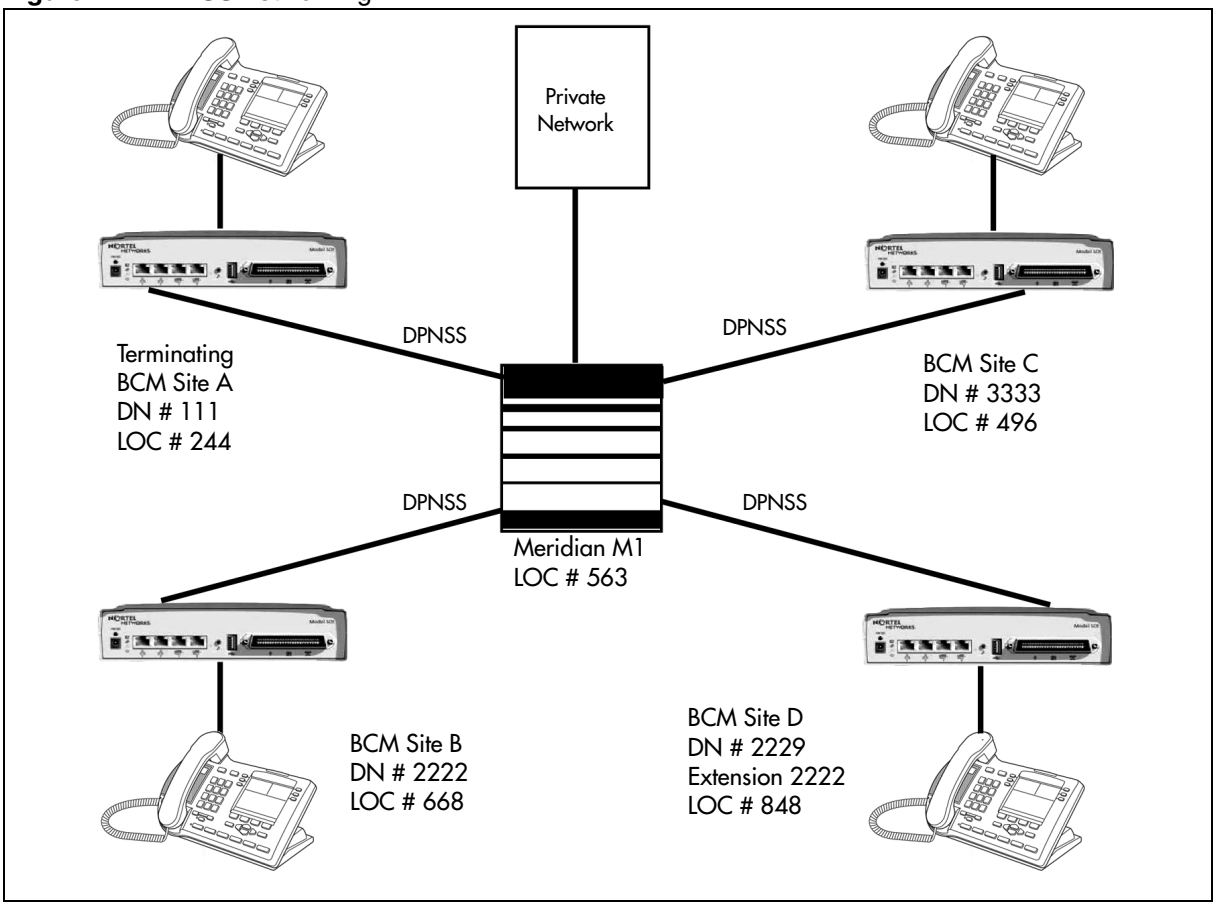
In this networking example, a private network is formed when several systems are connected through a Meridian 1 and a terminating BCM system. Each site has its own HLC and a range of DNs. Figure 11 illustrates this example.

Table 7 shows examples of the construction of numbers used when dialing within the example network. Note that 6 is the Private Access code.

Table 7 Calling numbers required for DPNSS network example

Calling Site	LOC/HLC	Calling Party Number	Called Site	Dialing String	Called Party Number
Site A	244	244 1111	Site B	6 668 2222	668 2222
Site B	668	668 2222	Site D	6 848 2222	848 2222
Site D	848	2222	Site D	2229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Figure 11 DPNSS networking



Calls are dialed and identified to the system as follows:

- To reach a telephone inside the Private Network, at the BCM site, dial the DN of choice.
- To reach a telephone inside the Private Network, from another site, dial HLC + DN.
- To reach a telephone outside the Private Network, dial an Access Code + HLC + DN.

  Each node has its own destination (dest) code, which includes the appropriate access and HLC codes to route the call appropriately.

BRI Euro Protocol

The Kapsch enhancement introduces two protocol types in BRI Euro Protocol.

- S-T user
- T-T user

The existing protocol type is renamed to S-T user.

Naming convention

Choose the protocol type for consistency with PRI trunk configuration. The PRI protocol type can be either User (Slave) or Network (Master). The BRI protocol type can be extended with T-T (Network). You can connect two BCMs through a BRI link.

S-T refers to a far end which has an S interface (Line in M1 terminology).

T-T refers to a far end which has a T interface (Trunk in M1 terminology).

In both cases, User is the user or slave end of the connection.

Application level differences

BRI Euro Protocol gives you the option to set the protocol type as S-T user or T-T user. The default setting is S-T user.

The S-T user type provides lines in Pool X mode, which already exist. If the far end interface is BRI loop choose the S-T user type. The T-T user type provides the lines in BlocX mode, which is newly introduced. If the far end interface is BRI trunk choose the T-T user type.

Protocol level differences

The following are the protocol level differences in the Kapsch enhancement:

- The S-T user type has the existing functionality which does not support PROGRESS_MESSAGE.
- The T-T user type supports PROGRESS_MESSAGE.
- After the destination telephone starts to ring in the S-T user, BCM does not send a message to the network.
- After the tandem occurs in the T-T user, BCM sends a message to the network.
- In the S-T user type, the BRI call is answered prior to the tandem, while in the T-T user type, the message is sent when the call is tandemed and answered only when the destination telephone answers the call.
- When the S-T user type is chosen, this can impact the billing in tandem cases. The billing metrics start once the call is tandemed and not when the destination telephone is answered. But in the case of the T-T user type, the billing is triggered when the far end answers the call and not when the call is tandemed.

Chapter 3
Telephony programming: Configuring call traffic

Telephony call traffic has a number of configuration requirements. Some configuration is common to both incoming and outgoing traffic. Other settings are specific to the call direction.

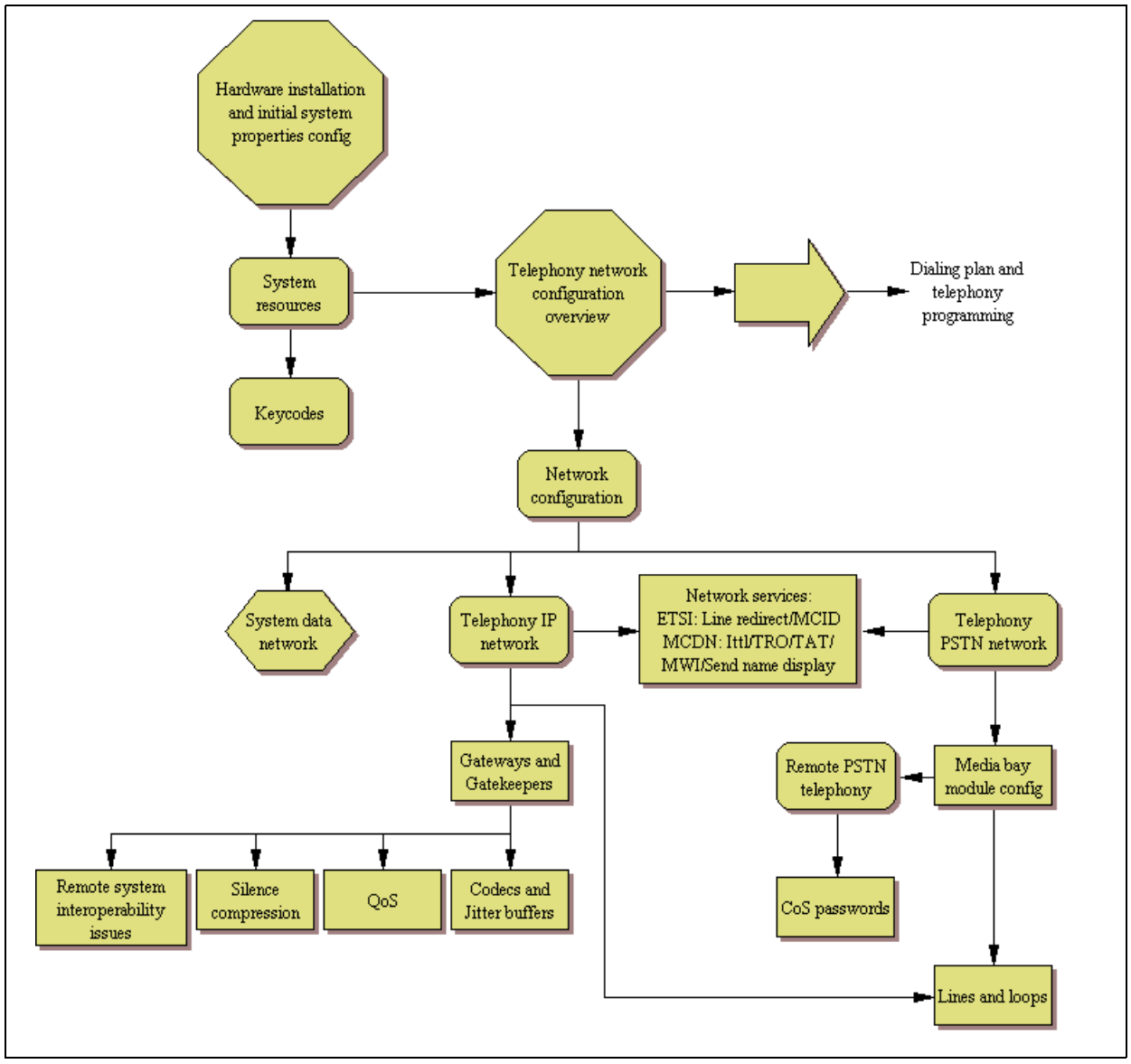
In the case of private networking, call configuration becomes more complex, as remote systems send calls over the private network to other nodes or to your system PSTN network and your local PSTN handles calls directed to remote nodes through your system.

Line programming and number planning both play critical roles in controlling call traffic for your system.

See also:

- "Incoming calls" on page 66
- "Outgoing calls" on page 70

Figure 12 Telephony system and device programming

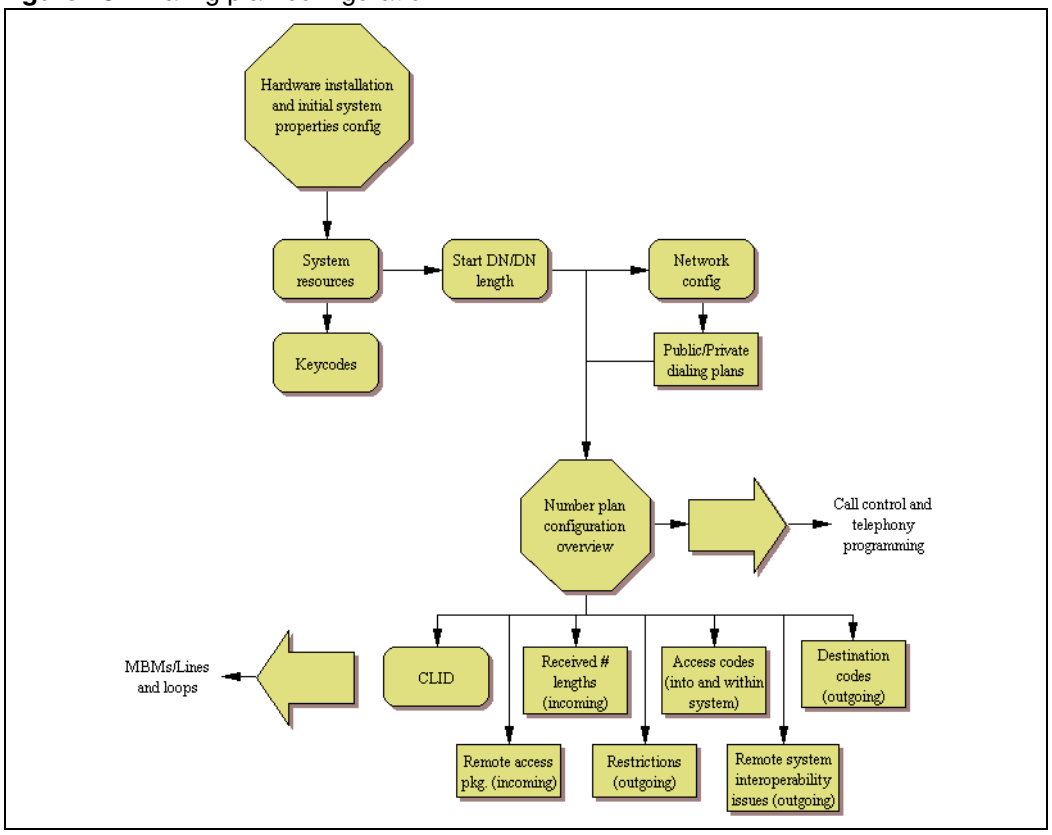


Although many of the tasks involved in programming both areas can be performed in any order, work flow falls generally in the following order:

- Module configuration/VoIP trunk gateways
  - "Configuring telephony resources" on page 101
  - "Managing modules" on page 87
  - "Module configuration: Trunk modules" on page 81
  - "Configuring VoIP trunk gateways" on page 381
  - "VoIP interoperability: Gatekeeper configuration" on page 389
  - "Setting up VoIP trunks for fallback" on page 391

- Line configuration/target line configuration
  - "BRI ISDN: BRI loop properties" on page 187
  - "BRI ISDN: BRI T-loops" on page 195
  - "Programming BRI S-loops, lines, and ISDN devices" on page 201
  - "Configuring BRI lines" on page 197
  - "Configuring lines" on page 129
  - "Configuring lines: T1-Loop start" on page 157
  - "Configuring lines: T1-E&M" on page 151
  - "Configuring lines: T1-Digital Ground Start" on page 163
  - "Configuring lines: T1-DID" on page 169
  - "Configuring lines: PRI" on page 145
  - "Configuring VoIP lines" on page 385
  - "Configuring lines: DPNSS lines" on page 181
  - "Configuring lines: Target lines" on page 141
  - "Call Security: Configuring Direct Inward System Access (DISA)" on page 427
- Networking, private and public
  - "Public networking: Setting up basic systems" on page 289
  - "Public networking: Tandem calls from private node" on page 293
  - "Private networking: Basic parameters" on page 315
  - "Private networking: MCDN and ETSI network features" on page 319
  - "Private networking: Using destination codes" on page 339
  - "Private networking: PRI Call-by-Call services" on page 343
  - "Private networking: PRI and VoIP tandem networks" on page 323
  - "Private networking: MCDN over PRI and VoIP" on page 297
  - "Private networking: DPNSS network services (UK only)" on page 331
  - "Configuring centralized voice mail" on page 351
- Dialing plan configuration

Figure 13 Dialing plan configuration



— “Dialing plan: System settings” on page 267
— “Dialing plan: Public network” on page 275
— “Dialing plan: Line pools and line pool codes” on page 357
— “Dialing plan: Routing and destination codes” on page 259
— “Dialing plan: Routing configurations” on page 247
— “Configuring CLID on your system” on page 205
— “Call security: Restriction filters” on page 433 (outgoing calls)
— “Call security: Remote access packages” on page 439 (incoming calls)

Incoming calls

For incoming calls, you can have a central reception point, or you can specify target lines to one or more telephones to receive directed calling.

You can arrange your telephones in Hunt groups, ringing groups, or call groups that use system-wide call appearance (SWCA) assignments to share calls.

You can also configure lines for use by system users who call in from outside the system. You can give them direct access to the system with an Auto DN, or you can configure the line so they hear a stuttered dial tone, at which point they need to enter a password (CoS) to gain access (DISA DN).

Figure 14 Incoming call configuration - part A

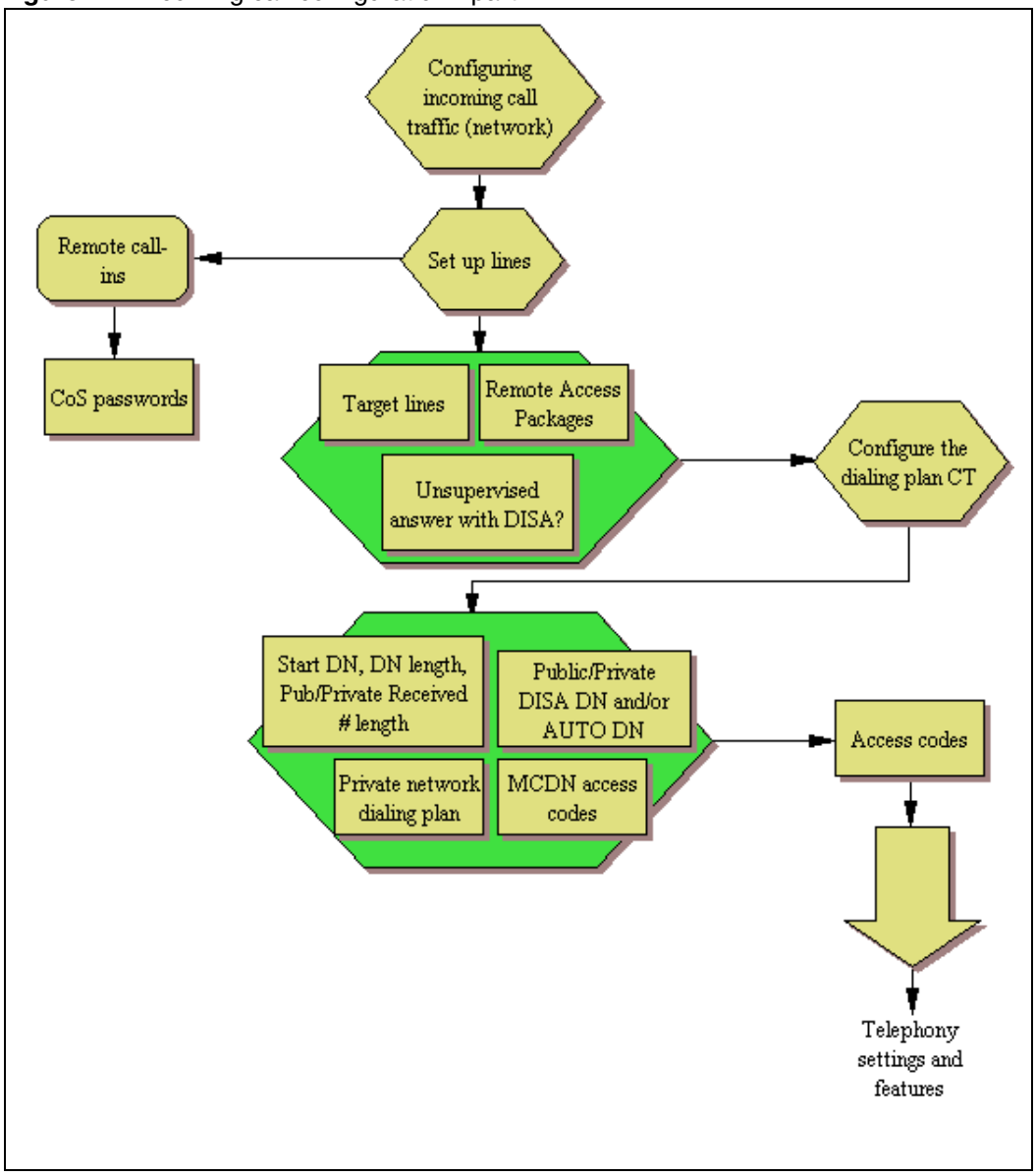


Figure 15 Incoming call configuration - part B

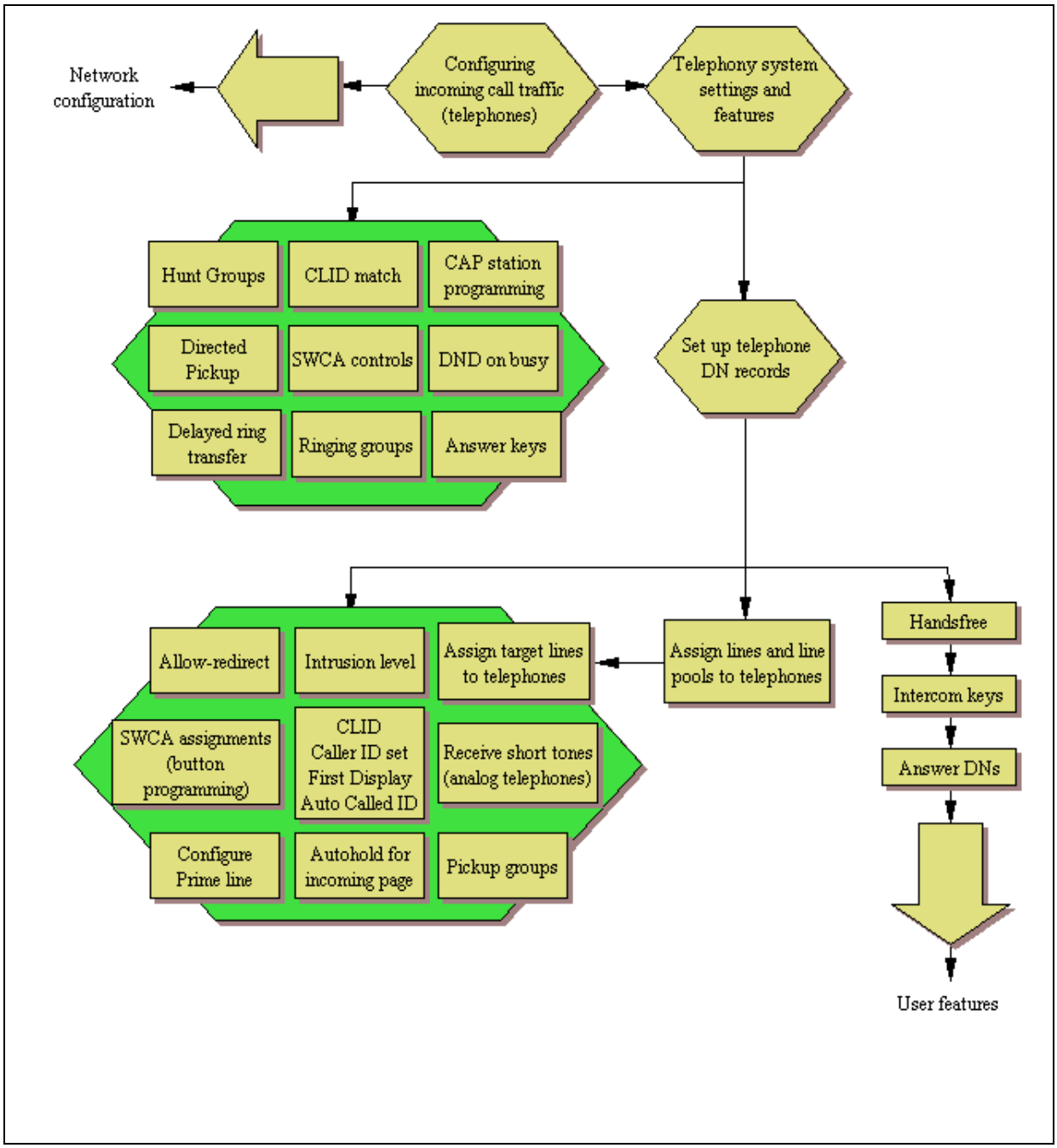
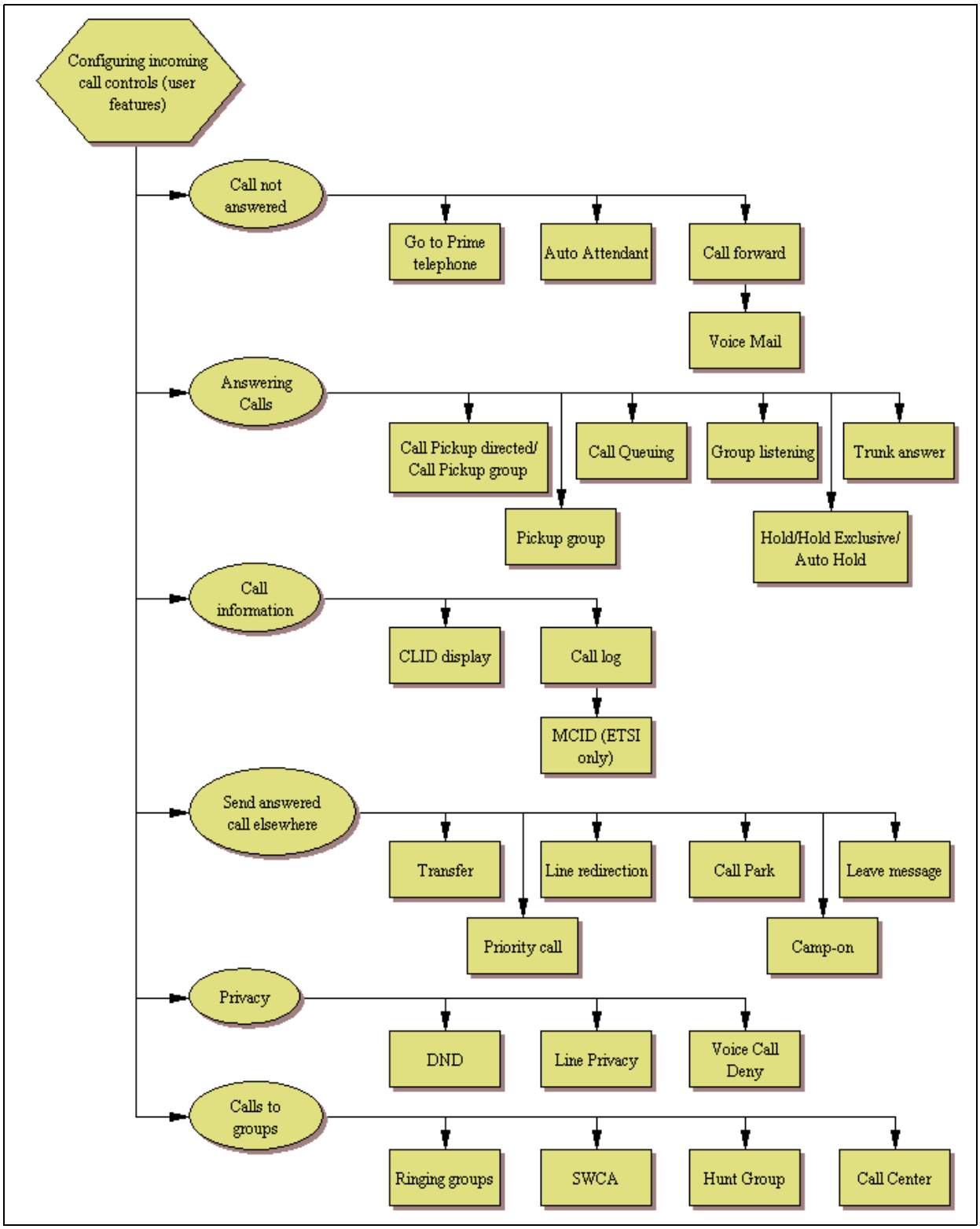


Figure 16 Configuring incoming call controls



Outgoing calls

For outgoing calls, you can assign one or more intercom keys to directly link to a line pool or prime line, or allow line pool access codes, destination codes, or internal system numbers to direct the call. Telephones without intercom keys on the telephone have intercom keys assigned, but the user must pick up the handset to access calls. In this case, the intercom key is an assigned DN.

For calls within the system, all telephones are virtually linked within the system. To call another telephone inside the system, lift the handset and dial the local DN. In this case, the prime line has to be set to intercom or none.

For calls going outside the system:

- If you assign the prime line to a line pool, all the lines in that line pool must be assigned to the telephone. When you pick up the handset, the telephone automatically grabs the first available line from the assigned line pool. In this configuration, you must ensure that the outgoing number is allowed by the line pool.
- If you assign the prime line to an intercom button, when you press the intercom button you get system dial tone. Then, you enter a line pool access code or a destination code to direct the outgoing call to the appropriate line pool, where it exits the system on any available line in that pool.

Figure 17 Configuring outgoing call traffic (Sheet 1 of 2)

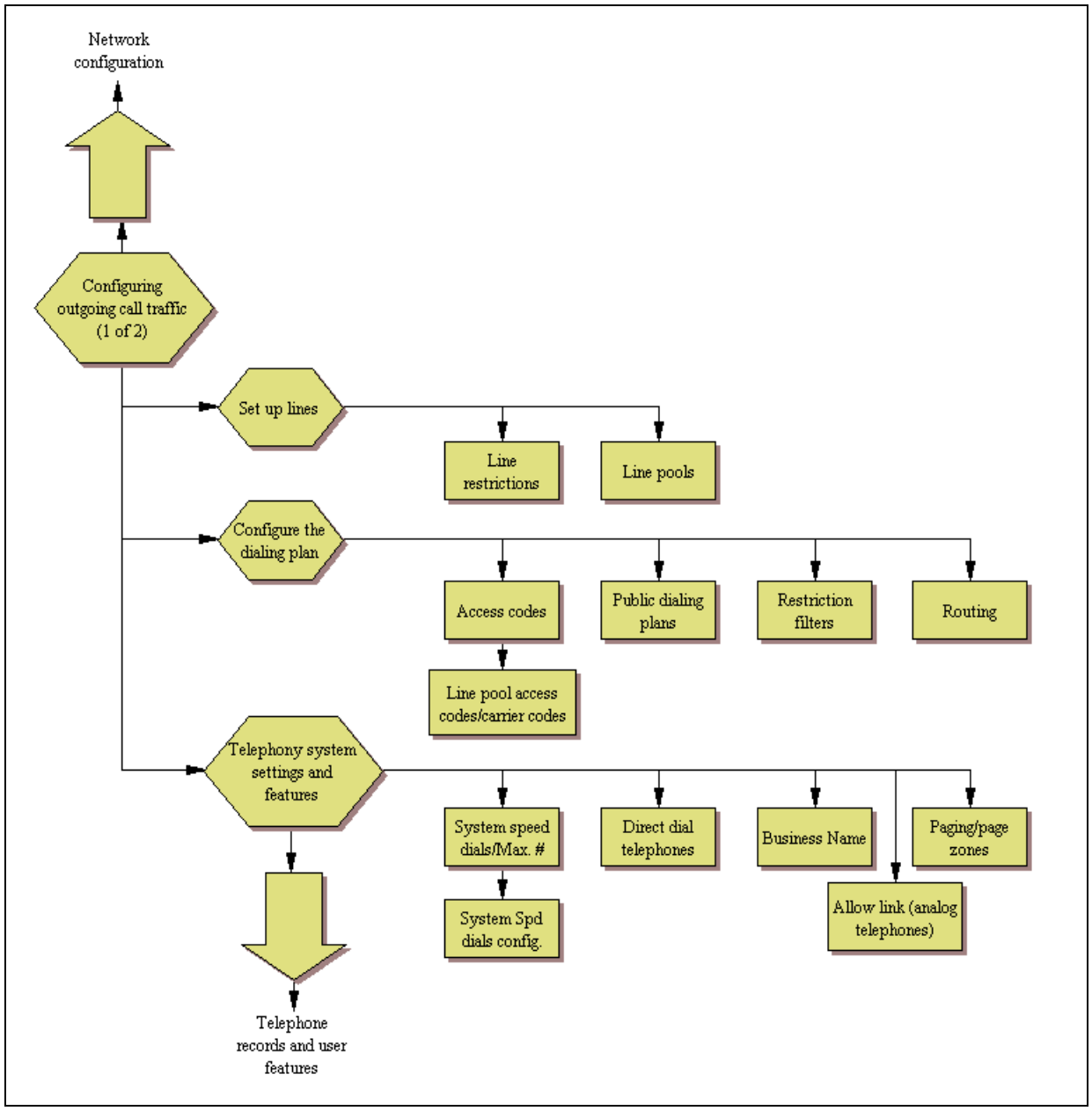
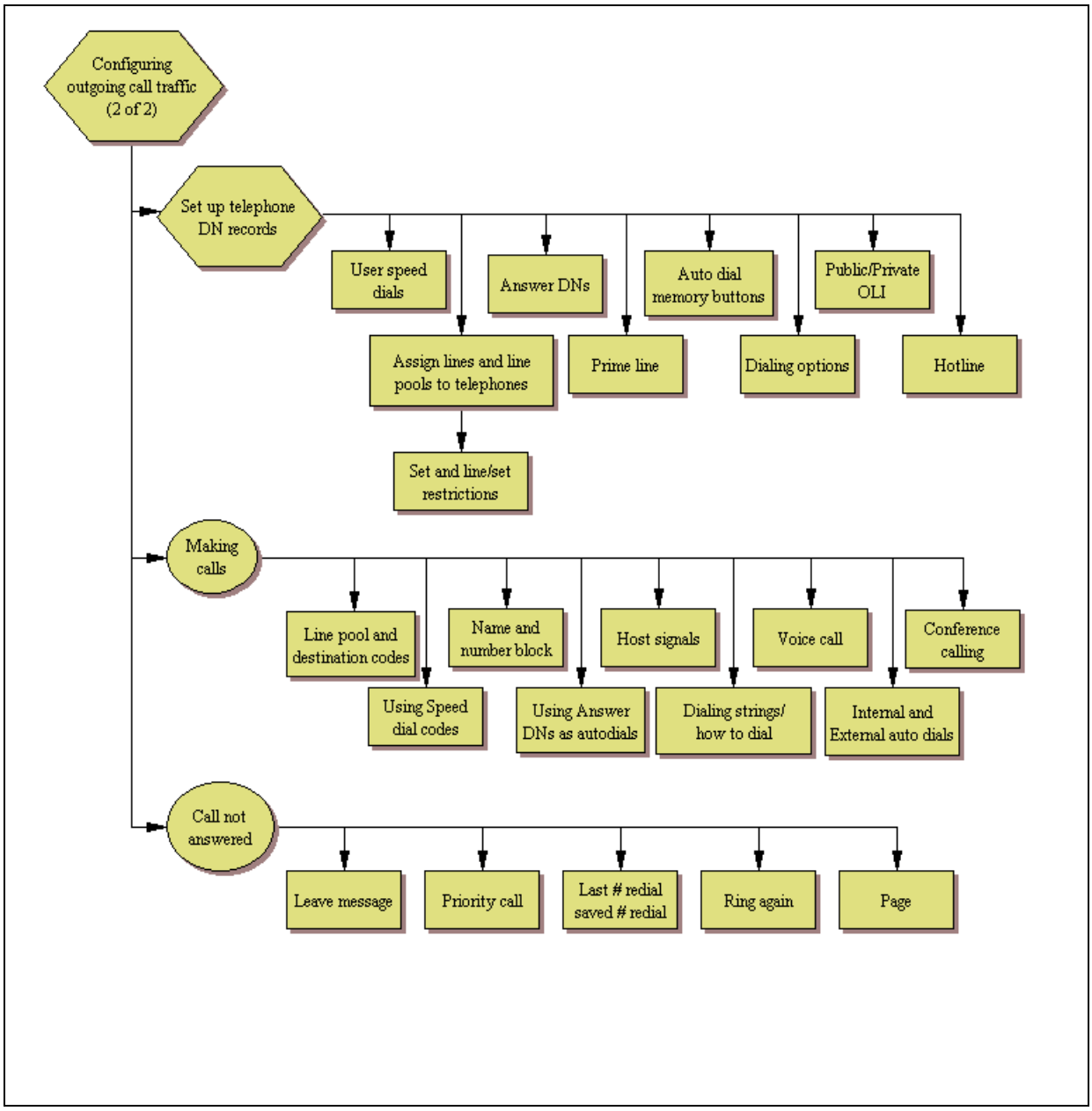


Figure 18 Configuring outgoing call traffic (Sheet 2 of 2)



Chapter 4
Application Resources overview

Application Resources is a management tool for allocating system resources such as signalling channels, VDI channels, media channels, and DSP resources. While the BCM manages resources for different services by making resources available as they are needed, you can manage the resources by setting minimums and maximums for each service.

For information on configuring application resources, see "Application Resources panel" on page 77.

Types of resources

There are four types of resources managed by the Application Resources panel:

- Signalling channels
- VDI channels
- Media channels
- DSP resources

Different applications require different resources. For example, each media gateway requires one DSP Resource and one media channel, but does not require any signalling channels or VDI channels. Use the Application Resources Reservations table to see what resources are required by each application. Whenever an entry contains N/A, the application does not use that resource.

Total and Reserved Resources

The total and reserved resource options display the current levels of total and reserved resources. The total resource table displays the total resources on the system, while the reserved resource table displays what resources are currently allocated or in use.

The total number of resources for signalling channels, VDI channels, and media channels exceeds the maximum capacity for the BCM, you do not need to manage the resources based on these channels. For example, IP Trunks are the only application that use VDI channels, and even if the BCM maximum of 12 IP trunks are in use, they will not exceed the total of 62 VDI channels. There is no need to modify the IP trunks minimum and maximum, since the necessary VDI resources will always be available.

The only resource you need to manage is DSP, which is used by media gateways, voice mail and Call Centre, Fax, and Conferencing.

Setting values for application resources

For all applications, you can modify the minimum and maximum values. The minimum values reflect the number of resources that will always be reserved for a particular application, while the maximum reflects the maximum instances of an application the system will allow at once. If an application attempts to use system resources and the system is already supporting the maximum for that application, the service will be declined, regardless of whether there are sufficient resources available. A value of MAX is also acceptable, which sets the maximum number of applications allowed to the maximum number possible. For example, the System Maximum for Media Gateways is 80. If the Maximum value for Media Gateways is set to MAX, then the system allows up to 80 Media Gateways at once, as long as sufficient resources are available.

Changes pending

In some cases, a change you make to the application resources panel may not be able to take effect immediately. For example, if you change the number of conference calls allowed from three to two, while there are three calls in progress, the resource allocations will not change until after one of the calls has been disconnected. In a situation where the changes cannot be made immediately, a checkmark appear in the Changes Pending box, and you can view details of these changes by clicking on the application and viewing the details below.

IP set resources

Because there is no circumstance where the number of IP sets on the system would exceed the available resources, there is generally no need to modify the resources for this application. However, if you want to limit the number of IP set connections, you can change the maximum value.

IP trunk resources

Because there is no circumstance where the number of IP trunks on the system would exceed the available resources, there is generally no need to modify the resources for this application. However, if you want to limit the number of IP trunk connections, you can change the maximum value.

Media gateway resources

Media gateways require DSP resources. Because there is often a slight delay in allocating the DSP resources, you may want to set the minimum to 2 or more. This will ensure that there is generally no delay in setting up the media gateway.

Voice mail and CC resources

These resources require DSP resources. Because there is often a slight delay in allocating DSP resources, you may want to set the minimum to 2 or more. This setting generally ensures that there is no delay occurs in setting up the application.

Fax

Fax has a maximum of 2. Each fax uses three DSP resources, so if you find that your system is always running low on resources, you may want to limit fax to 1.

Conf. Parties

The total number of parties across all simultaneous conferences cannot exceed 18, and a single conference can contain up to 18 parties.

Conf. Mixers

A conference mixer allows several conference parties to be mixed into a conference. BCM supports up to 9 simultaneous conferences.

SIP Trunks

Because there is no circumstance where the number of SIP trunks on the system would exceed the available resources, there is generally no need to modify the resources for this application. However, if you want to limit the number of SIP trunk connections, you can change the maximum value. BCM supports a maximum of 12 SIP trunks.

Digital Trunks

Because there is no circumstance where the number of digital trunks on the system would exceed the available resources, there is generally no need to modify the resources for this application. However, if you want to limit the number of digital trunk connections, you can change the maximum value. BCM supports a maximum of 2 digital trunks.

Chapter 5
Application Resources panel

The application resources panel allows you to modify resources allocated to applications on the BCM. While the panel tracks four types of resources, DSP resources are generally the only type of resources that affect performance on the BCM. For more information on planning your application resources, see "Application Resources overview" on page 73.

Note: Do not change these settings unless you want to restrict resources.

The application resources panel consists of three tables and a panel:

- Total Resources
- Reserved Resources
- Application Resource Reservations
- Details for application

Total Resources

The total resources options show the maximum resources available for each type of resource.

Reserved Resources

The Reserved Resources options show the resources currently reserved or in use.

Application Resource Reservations

Use the Application Resource Reservations table allow you to set minimum and maximum values for telephony resources. The table contains 10 columns, 8 of which are read-only. For information about determining the appropriate values for each type of application, see "Setting values for application resources" on page 74.

Details for application

The Details for Application panel changes whenever you select a different row from the Application Resource Reservations table. The panel reflects the current minimum and maximum limits, in instances where changes do not happen immediately.

Figure 19 Application resources panel

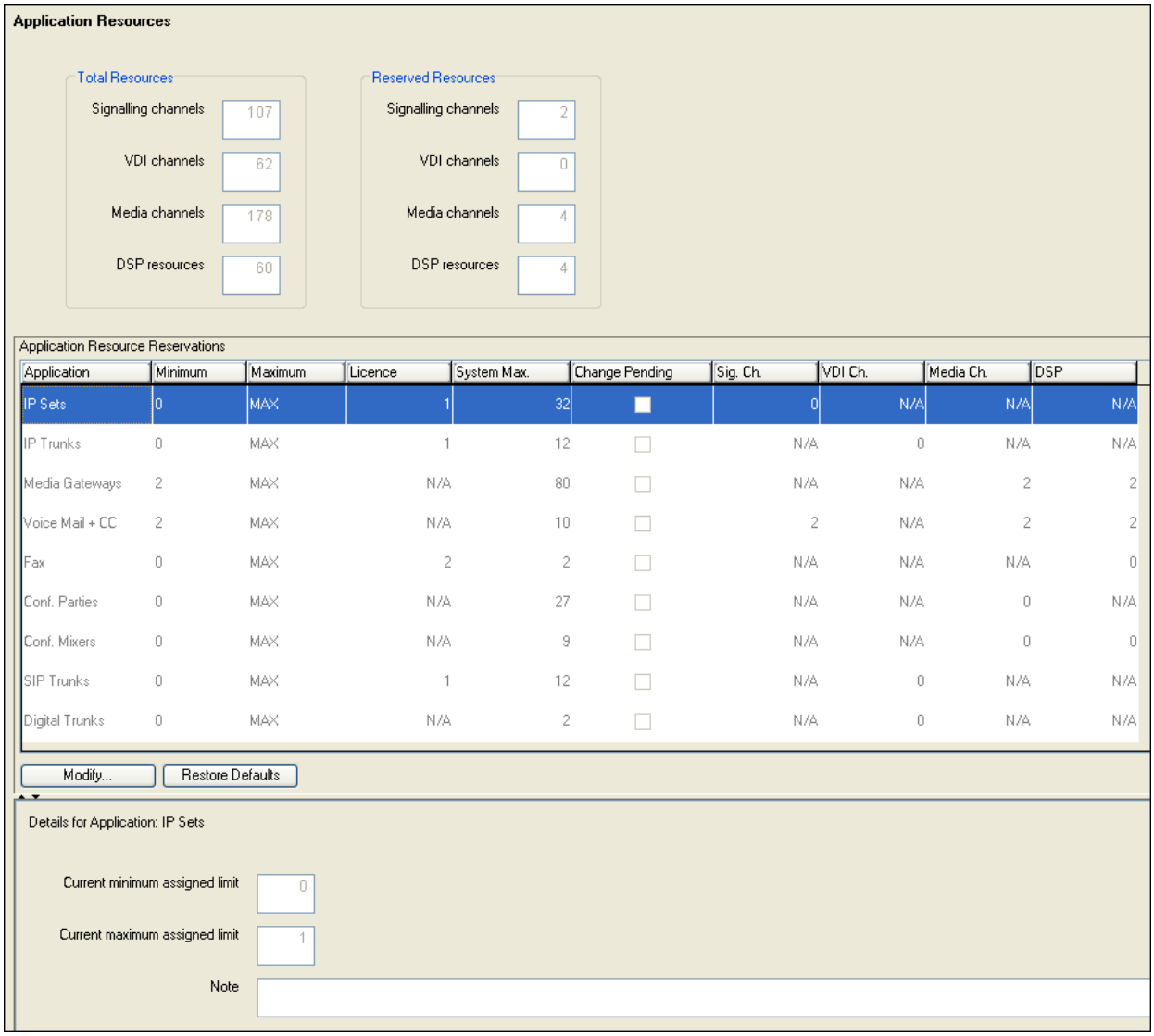

Application Resources
Total Resources
Signalling channels 107
VDI channels 62
Media channels 178
DSP resources 60
Reserved Resources
Signalling channels 2
VDI channels 0
Media channels 4
DSP resources 4
Application Resource Reservations
Application Minimum Maximum Licence System Max. Change Pending Sig. Ch. VDI Ch. Media Ch. DSP
IP Sets 0 MAX 1 32 0 N/A N/A N/A
IP Trunks 0 MAX 1 12 N/A 0 N/A N/A
Media Gateways 2 MAX N/A 80 N/A N/A 2 2
Voice Mail + CC 2 MAX N/A 10 2 N/A 2 2
Fax 0 MAX 2 2 N/A N/A N/A 0
Conf. Parties 0 MAX N/A 27 N/A N/A 0 N/A
Conf. Mixers 0 MAX N/A 9 N/A N/A 0 0
SIP Trunks 0 MAX 1 12 N/A 0 N/A N/A
Digital Trunks 0 MAX N/A 2 N/A 0 N/A N/A
Modify...
Restore Defaults
Details for Application: IP Sets
Current minimum assigned limit 0
Current maximum assigned limit 1
Note

Table 8 Application Resources panel (Sheet 1 of 3)

Attribute	Value	Description
Total Resources		
Signalling channels	<read-only>	The total number of signalling channels on the system.
VDI channels	<read-only>	The total number of VDI channels on the system.
Media channels	<read-only>	The total number of media channels on the system.
DSP resources	<read-only>	The total number of DSP resources on the system.
Reserved Resources		
Signalling channels	<read-only>	The number of signalling channels in use on the system. This number can change based on the values entered for applications, and on the those applications currently in use.

Table 8 Application Resources panel (Sheet 2 of 3)

Attribute	Value	Description
VDI channels	<read-only>	The number of VDI channels in use on the system. This number can change based on the values entered for applications, and on the those applications currently in use.
Media channels	<read-only>	The number of media channels in use on the system. This number can change based on the values entered for applications, and on the those applications currently in use.
DSP resources	<read-only>	The number of DSP resources in use on the system. This number can change based on the values entered for applications, and on the those applications currently in use.
Application Resource Reservations		
Application	<read-only>	The name of the application.
Minimum	<numeric value>	The minimum number of resources reserved at all times for the application. If a value of 2 is entered, the system will always reserve enough resources for 2 instances of the application.
Maximum	<numeric value, or the string MAX>	The maximum number of applications to allow. If the value is set to MAX, the system will allow up to the system maximum, as long as there are enough resources.
Licence	<read-only>	The number of licenses the system has activated for the application. If the value is N/A, the application does not require licenses.
System Max.	<numeric value>	The maximum instances of an application the BCM can support.
Change Pending	<read-only>	If this box is selected, a change is pending to the system. Most changes take effect immediately, but in some instances, a change may wait until applications shut down. Details about changes pending can be seen in the details panel.
Sig. Ch.	<read-only>	The number of signalling channels reserved by the application. This can be changed by modifying the minimum and maximum values for the application. If the field has a value of N/A, the application does not require this type of resource.
VDI Ch.	<read-only>	The number of VDI channels reserved by the application. This can be changed by modifying the minimum and maximum values for the application. If the field has a value of N/A, the application does not require this type of resource.
Media Ch.	<read-only>	The number of media channels reserved by the application. This can be changed by modifying the minimum and maximum values for the application. If the field has a value of N/A, the application does not require this type of resource.
DSP	<read-only>	The number of DSP resources reserved by the application. This can be changed by modifying the minimum and maximum values for the application. If the field has a value of N/A, the application does not require this type of resource.

Table 8 Application Resources panel (Sheet 3 of 3)

Attribute	Value	Description
Details for Application		
Current minimum assigned limit	<read-only>	The current minimum assigned for an application.
Current maximum assigned limit	<read-only>	The current maximum assigned for an application.
Note	<read-only>	Indicates any pending changes.

Chapter 6
Module configuration: Trunk modules

This following describes the Element Manager headings that define and control the settings for the trunk media bay modules installed on your system.

The following paths indicate where to access the trunk modules in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Resources > Telephony Resources**
- Telset interface: ****CONFIG > Hardware**

For an overview of the Telephony Resources panel, refer to "Configuring telephony resources" on page 101.

Task: To confirm settings for the trunk media bay modules installed in the system.

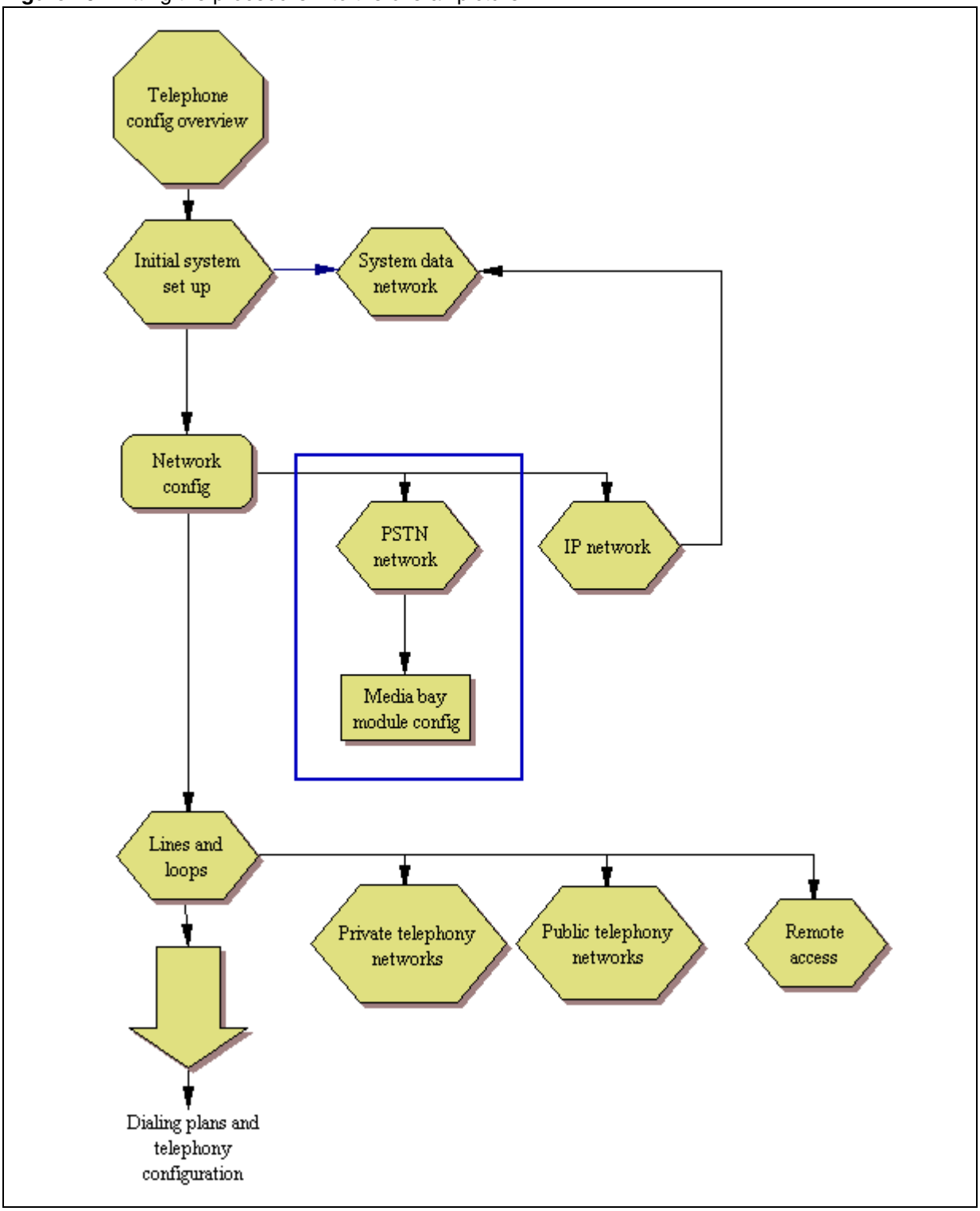
- Confirm that all prerequisites are complete. Refer to "Configuring the trunk module parameters" on page 83.
- Confirm or set module parameters as follows:
  - If your module supports T1, PRI, or DASS2, refer to "Call-by-Call Service Selection" on page 108 and "Provisioning module lines/loops" on page 112.
  - For other types of trunk modules, configure each line record. Refer to "Configuring lines" on page 129.
- Provision modules and confirm auto-entry information. Refer to "Provisioning module lines/loops" on page 112.

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

System hardware is installed and operating correctly.	
All relevant central office/service provider information for the trunk type has been obtained.	
Keycodes have been activated for core module trunks.	
Expansion modules are installed and operating, and LEDs are correct.	

Figure 20 Fitting the procedure into the overall picture



Configuring the trunk module parameters

Modules automatically configure to a free bus when they are connected to the system.

- That bus determines what line numbers are supported by the module.
- Module programming determines the type of line.
- Trunk configuration determines the line properties for the system.

To define the modules to the system

1. On the Modules panel, click the trunk module entry that you want to view.
2. On the Module Parameters tab panel, review the settings to ensure they support the type of line function provided from the Central Office (CO). For details of the configurable parameters for a trunk type, refer to "Module parameters list" on page 83.
3. If your module supports T1, PRI, or DASS2, refer to "Call-by-Call Service Selection" on page 108 and "Provisioning module lines/loops" on page 112.

   If your module supports other types of trunks, configure each line record. Refer to "Configuring lines" on page 129.

Module parameters list

The following contains information about the module parameters that are specific to a module type.

Refer to "Trunk Module Parameters" on page 104 for detailed field descriptions.

Configuring digital and analog loop module parameters

- Module mode: The mode for the type of line being supported (DS/CLID, Global, Legacy).
- Disconnect Timer: Enter the time delay for disconnect supervision for lines supplying supervised external lines. This setting must match the CO setting.

Configuring DTM-T1/E1 module parameters

- Clock Source: Determine how the module functions for timing on the network (Primary External, Secondary External, Internal).

Warning: Changing the clock source may disconnect calls.
If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

- CO fail: Use the carrier failure standard used by the service provider (TIA-5474, TR62411).
- Interface levels: Choose the loss plan setting supported on the lines (ISDN, PSTN).
- Framing: Choose the framing format supported by the service provider (ESF, SF).
- Internal CSU: Turn the internal channel on or off.

Warning: Disable the module before changing the internal CSU setting.

- CSU line build (Internal CSU set to ON): Set the gain level of the transmitted signal (0, 7.5, 15 dB)
- DSX1 build (Internal CSU set to OFF): Set the distance between the system hardware and the external channel service unit (000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet)
- Line coding: Select the encoding signal used by the service provider (B8ZS, AMI)
- CRC4 (E1 lines only): Set the parameter to match the setting at the other end of the line.

Configuring DTM-PRI module parameters

- Protocol: Set to the protocol used by the CO.

Warning: Always confirm the line protocol with the head office. Failure to set the correct protocol could result in erratic service or service failure on the lines.

PRI-T1 supports: NI-2, DMS-100, DMS-250, 4ESS, SL-1

PRI-E1 supports: ETSI QSIG, Euro, SL-1

Note: SL-1 and ETSI QSIG require an MCDN keycode.

- Protocol type (for SL-1): Select the setting that applies to the way in which the system is viewed by the network. Default is User (Slave) (the CO or another network node controls the network).
  If you want this system to control the network protocol, select Network.

- NSF Extension: None (DMS-100/250 switches); WATS (Siemens, ESWD, Lucent 5ESS switches); ALL (GTD5 and DMS-10 switches).
- B-channel selection sequence: choose how B-channel resources are selected for call processing.
- Clock Source: Determine how the module functions for timing on the network (Primary External, Secondary External, Internal)

Warning: Changing the clock source may disconnect calls.
If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

- Send Name Display: select check box to activate outgoing name display (OLI).
- Remote Capability MWI (SL-1): Select the check box only if connecting to a Meridian 1, or other compatible endpoint, with the appropriate MWI package and RCAP set to MWI.
- Maximum transits (SL-1): Default: 31. Set the number of times a call will be transferred within the private network before being dropped.
- CO fail: Use the carrier failure standard used by the service provider (TIA-5474A, TR62411)
- Interface levels: Choose the loss plan setting supported on the lines (ISDN, PSTN)
- Framing: Choose the framing format supported by the service provider (ESF, SF)
- DSX1 build (Internal CSU set to OFF): Set the distance between the system hardware and the external channel service unit (000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet)

Configuring BRI Loop module parameters

- Clock Source: Determine how the module functions for timing on the network (Primary External, Secondary External, Internal). When the BRI module is configured as a T-loop this parameter is configured under **Configuration > Telephony > Loops**.

Warning: Changing the clock source may disconnect calls.
If you change the clock source for your system, you may cause your system BRI S/T interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

- Send Name Display (BRI-QSIG): select check box to activate outgoing name display (OLI). When the BRI module is configured as a T-loop this parameter is configured under **Configuration > Telephony > Loops**.

Configuring DASS2 module parameters

- Clock Source: Determine how the module functions for timing on the network (Primary External, Secondary External, Internal)

Warning: Changing the clock source may disconnect calls.
If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.

Configuring European DTM/DPNSS line parameters

- Host node: Choose the type of switch the lines connect to, to ensure correct call forwarding (M1, Embark, IDPX, DSM).

Chapter 7
Managing modules

When you need to find out information about a module, you can determine the status of any of the settings under the media bay module headings. To correct a problem or change a module setting, you may need to enable or disable a bus/module or select ports on the module. Refer to the following procedures:

- "Disabling or enabling a bus or module" on page 87
- "Disabling or enabling a port channel setting" on page 87
- "Trunk module metrics" on page 88

Disabling or enabling a bus or module

The following procedure describes the process for enabling or disabling a bus. This means that if there is more than one module assigned to the DS30 bus, all modules will be disabled.

To enable or disable a bus

1. Click **Configuration > Resources > Telephony Resources > Modules** panel, and then click the module you wish to enable or disable.
2. Click either **Enable** or **Disable**.
   The system prompts you to confirm your request.
3. Click **OK**.

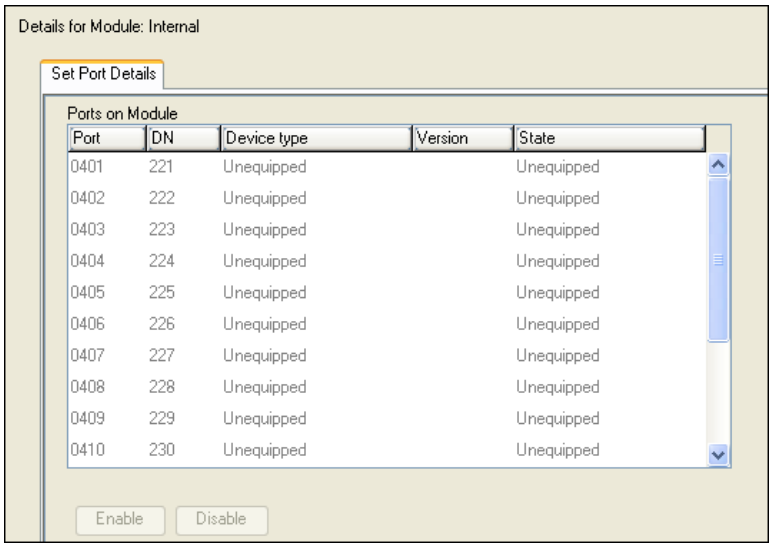
Disabling or enabling a port channel setting

If you need to isolate a problem or block access from the module, you may need to turn off individual port channels, rather than the entire module.

To turn a port channel on or off

1. Click **Configuration > Resources > Telephony Resources > Modules** panel, and then click the module supporting the port you want to enable/disable.
2. Select the port you want to enable/disable in the Set Port Details tab.
3. Click either the **Enable** or **Disable** button.
   The **State** field indicates the mode of operation for the port, as shown in Figure 21. If the port is enabled, this field shows unequipped unless a device is physically connected.

Figure 21 Set Port Details



Note: A trunk media bay module has no changeable settings on the Trunk Port Details record.

Trunk module metrics

To view the current status of the module trunks, you can use the Telephony Metrics – Trunk Modules Metrics panel. See the *Administration Guide* (NN40020-600) for more information about telephony metrics.

Chapter 8
Lines overview

Telephony signals into the system, within the system, and out of the system are carried over channels. For consistency, these channels are all called lines or trunks. This designation includes:

- circuit switched lines (PSTN): connect to the system through media bay modules
- Voice over IP (VoIP) trunks: connect through the LAN or IP network
- target lines, internal channels: connect PRI, T1 and VoIP trunks to specific devices
- intercom lines: connect all internal telephones together through the DN numbers, and allow the user to access line pools for making outgoing calls, as well as being required for other call features such as conference calling and system-wide call appearance (SWCA) calls. Intercom designations are assigned in the DN record, or automatically by the system for each telephone.

Prerequisites

You must configure the media bay modules and/or the VoIP trunk parameters before you can set up line programming.

- The position on the system bus of the trunk media bay modules determines the line numbers that are available. See the *Installation and Maintenance Guide* (NN40020-302).
- The position on the system bus of the station media bay modules determines which DNs are available, although DN numbers can be changed.
- Available VoIP lines are determined by the number of VoIP keycodes entered on the system (between 01 and 12), starting with line 001 and ending at line 012.

See the following information:

- "Understanding how the system identifies lines" on page 90
- "Line record" on page 93
- "Line Job Aids" on page 94

Other line configuration options or requirements:

- **BRI loops** require configuration and provisioning before the BRI lines can be configured.
- The BCM50 does not support the DDIM (Digital Drop Insert MBM).

Understanding how the system identifies lines

On a new system, lines and loops are numbered and assigned defaults based on the type of media bay modules that have been connected to the system. The exception are the VoIP trunks, which require a keycode to activate.

These panels allow you to easily view which lines have been enabled through a media bay module.

From this heading, you can access each line record and assign attributes, as you require.

Determining which lines you need to program

Under **Lines**, note that line types are divided into five headings. The fifth heading contains all line numbers.

- "Active physical lines"
- "Active VoIP lines (require keycode)"
- "Target lines" on page 91
- Inactive Lines
- All Lines

Active physical lines

Lines 061-124 are reserved for physical lines.

Active VoIP lines (require keycode)

Voice over IP (VoIP) lines are signaling channels that simulate how CO lines work. However, VoIP lines transmit data to the IP network over a LAN or IP network rather than over physical lines. Once the VoIP trunks are set up, you can assign them to line pools, and program their behavior in the same way you would PRI lines.

VoIP lines use line numbers 001 to 012. These line records appear under **Configuration > Telephony > Lines > Active VoIP Lines**. To access VoIP lines, you need to enter software keycodes. Each keycode supports a specific number of lines. No entries appear in the Enabled VoIP lines field until you complete the IP Trunks Settings field, which appears when you click IP Trunks under **Configuration > Resources > Telephony Resources > IP trunks**.

VoIP trunks should be configured to use a single line pool per trunk type. Do not mix other trunk types on the same line pool. The VoIP line pools are assigned to routes, which, in turn, are configured with destination codes that route calls to the designated remote gateways of other BCM systems or Succession, or MCS5100 systems.

You can also create a fallback for the trunk. This is a situation where the system reroutes the call to a PSTN line pool if the primary route is not available or the call quality is not suitable. If you do not configure your network for fallback and the call quality is below threshold, the IP call fails.

Target lines

Target lines are internal communications paths that directly connect auto-answer trunks to system telephones. These lines are incoming only.

Target lines allow you to make more efficient use of DID line resources.You can map a range of target lines for each DID line. The incoming call is routed according to the mapped dialed digits, rather than a one-to-one line assignment. Systems configured using the DID template automatically assign target lines to all assigned DNs.

You also require target lines when you use PRI, T1 or VoIP trunks.

Target lines use line numbers 125 to 268. To view these lines, select **Configuration > Telephony > Lines > Target Lines**. Record this information in your system Programming Records so you have a clear view of where each line is assigned.

Other features:

- Each target line can be assigned to more than one telephone.
- A telephone can have multiple appearances of a target line.

Target lines are internal direct links the BCM uses to allow external callers to dial specific system telephones or a group of system telephones. You assign the target line to one or more telephone DNs, and then configure the target line to function as you require. You can also assign multiple appearances of a target line to one telephone. This allows more than one call to simultaneously use the target line. Target lines are required by lines that support multiple numbers over one trunk (T1 E&M, DID trunks, T1 DID trunks, PRI trunks, and VoIP trunks).

Caution: Changing the received # length:
If you change the received # length for your system, the **Public number** entry for the target lines will clear if the new received # length is less than the number entered in this field.
If the new received # length has more digits than the number entered in this field, you need to change the entry manually, if changes are required.

Programming note: The following trunks use one or both of these settings to route calls:

- DPNSS lines use the Private received number to route calls in the system.
- BRI ETSI-QSIG, PRI ETSI-QSIG, MCDN, DMS-100, DMS-250, and VoIP trunks route calls on a per-call basis to either the public or private received digits.

Note: VoIP trunking MCDN calls do not support Auto DN/DISA DN functionality.

- BRI (ETSI-Euro, NI), PRI (ETSI-Euro, NI, 4ESS), T1 (LoopStart, E&M, DID, GroundStart), Analog LEC (LoopStart), and DASS2 trunks route calls using the Public received number.

Physical lines

Physical lines are the central office (CO) trunks assigned to the trunk media bay modules. See the *Installation and Maintenance Guide* (NN40020-302) for information about which lines are enabled.

You can change the line types to suit your system. For instance, BRI and DTM modules can be designated to a number of line types, depending on the type of line service provided through the central office (CO). However, the line numbers are associated for specific tasks or to specific DS30 bus numbers.

The line record allows you to program settings for lines that affect how the lines operate in the network and with other switches, as well as how the system uses the line.

Trunk types:

- VoIP
- DTM (digital): TI types (Loop, E&M, DID, Ground, or fixed data channel), PRI, DASS2, DPNSS.
- CTM (North America)/GATM: Analog Loop
- BRI: BRI S/T
- Target lines

BRI loops programming

The Loops panels define the loop numbers and loop attributes that correspond to the DIP switch settings that were configured on the BRI trunk media bay modules installed on your system. Check your Programming Record to see which modules are installed, and what settings were chosen.

Available BRI trunk loop attributes are determined by the country profile that is assigned to your system. All profiles allow BRI programming; however, there is a difference between T1-based profiles and for E1-based profiles.

Once loops are provisioned, the system assigns two line numbers per loop. These lines are then programmed as you would any other lines.

You can program a loop to support either trunking services to the ISDN network, or terminal services to one or more ISDN devices. The following sections describe the programming for each type of loop. For complete module installation instructions and safety precautions, see the *Installation and Maintenance Guide* (NN40020-302).

Programming links

Determine line assignments for routing: “Line Job Aids” on page 94.

Line record

The line record allows you to:

- Identify the line and the features on the line.
- Assign restrictions for outgoing calls.
- Assign a voice message center, if the line connects to a remote voice-mail system, either on another node on the private network or at the central office.

Line characteristics

Line type determines what features are available. Some features must be coordinated with the settings at the other end of the line.

Programming links

Alternate-click the Line Assignment panel tab to see a list of the line feature settings, and to see which lines have each setting.

Line restrictions

Restrictions prevent certain kinds of calls from occurring over specific lines. You can also restrict some features.

If you want different restrictions to apply at different times of the day or week, you can set up the line restriction schedules to that effect. The Normal schedule runs when no other schedule is specified or if fallback is used for VoIP trunks.

The default restriction filters are listed in Table 9.

Table 9 Default restriction filters

Schedule	Use filter
Normal	03
Schedule 1 (Night)	21
Schedule 2 (Evening)	22
Schedule 3 (Lunch)	23

Schedule	Use filter
Schedule 4	00
Schedule 5	00
Schedule 6	00

Note: When a remote user places an external call on a line, any filters used with the line still apply.

Programming links

The template has a set of default restrictions in Restriction 02 only. You must create your own restriction files if you want to use other settings.

Remote restrictions

Your system can accommodate users who call in from outside the system to access system features. Calls coming in over the Private network that are routing out of the system to remote systems or to the PSTN are also considered to be remote call-ins.

To restrict the access remote callers have, or to control outbound private network calls, specify the appropriate filter for the line.

If you want different restrictions to apply at different times of the day or week, you can set up the line restriction schedules to that effect. The Normal schedule runs when no other schedule is specified or if fallback is used for VoIP trunks.

The default restrictions are shown in Table 10

Table 10 Default remote restrictions

Schedule	Restriction filter	Schedule	Restriction filter
Normal	04	Schedule 4	00
Schedule 1 (Night)	31	Schedule 5	00
Schedule 2 (Evening)	32	Schedule 6	00
Schedule 3 (Lunch)	33		

Note: The remote restriction restricts the numbers a user can dial on an incoming auto-answer line. If a remote user then selects a line to place an external call, any filter used with the line still applies.

Voice message center

If you subscribe to a voice message service outside your office, you can indicate to the line with which voice message service to connect.

Voice message centers are defined as part of the system telephony global programming. This is located in the Element Manager under **Configuration > Applications > Voice Messaging/ Contact Center**.

Line Job Aids

See the following additional information:

- “Determining line numbers and destination codes” on page 95
- “Line pool tips” on page 96

- "Using loss packages" on page 97
- "Turn Privacy on or off for a call" on page 98

Determining line numbers and destination codes

Refer to Table 11 for a list of lines assigned per bus (DS30 bus and offset), based on the module type configured with that address. You can use this chart to note which lines should be active for the modules you installed. You can also note which line pool you put the lines in, and note the line pool access codes or routes and destination codes to which you assigned the line pools (or use your programming records).

Follow these steps to use the table:

1. For each bus number, circle the module you set to that number.
2. Beside the module name, circle the group of line numbers appropriate for the offset you set on the modules.
3. In the Line pool column, indicate a line pool name if you want to associate lines into a pool. This enables assigned telephones to grab any free line from the pool.
4. On the far right column, list the access codes and routes associated with the lines.

Table 11 Line numbering for modules and VoIP

DS30 bus	Type of module	Line/Loop numbers (default)				Line pool A-O/Bloc	Access codes and routes
N/A	VoIP trunks (no module)	001-048					
3	Integrated BRI loops (2)	061-064					
05 /06	**Expansion 1**						
	DID4	65-68					
	DID8	65-76					
	DTM (T1)	65-88					
	DTM (NA-PRI)	65-87					
	DTM (E1 PRI)	65-94					
	BRI	65-72					
	CTM4, GATM4 and **4X16**	65-68					
	CTM8, GATM8, 8X16 (upper/lower)	65-68 73-76					
	ISDN loops						
	BRI ST	365-380					
07/08	**Expansion 2**						
	DID4	95-98					
	DID8	95-106					
	DTM (T1)	95-118					
	DTM (NA-PRI)	95-117					
	DTM (E1 PRI)	95-124					
	BRI	95-102					
	CTM4, GATM4 and **4X16**	95-98					
	CTM8, GATM8, 8X16 (upper/lower)	95-98 103-106					
	ISDN loops						
	BRI ST	381-396					

Line pool tips

Line pools are groups of lines. Pooling lines allows you to use fewer lines than there are users. PRI lines and VoIP lines are always defined into line pools.

- Line pools must never contain a mixture of lines. All lines in a given line pool should go to the same location.

- Avoid putting unsupervised loop start lines in a line pool. These lines can become unusable, especially when a remote user uses the line pool to make an external call.
- To assign line pool access to telephones, select **Configuration > Telephony > Dialing Plan > Line Pools**.
- To assign system-wide line pool access codes, select **Configuration > Telephony > Dialing Plan > General** (not applicable to Bloc pools).
- A telephone can be administered to search automatically for an idle line from several lines that appear on the telephone. Assign a line pool as the prime line. When the user lifts the receiver or presses Handsfree, any one of the lines, if idle, can be selected by Automatic Outgoing Line selection.
- Changes in the settings for trunk type on a system that is in use can result in dropped calls.
- When assigning lines to line pools, consider your network configuration. You can create a unified dialing plan by assigning lines to the same location to the same line pool on each of your systems. For example, if system A and system B each have TIE lines to system C, assign the TIE lines to pool D on each of the systems. You cannot assign target lines to a line pool, as they are incoming-only.

Using loss packages

Use the loss package settings to select the appropriate loss/gain and impedance settings for each line. The setting is based on the terminating switch type and the distance between BCM and the terminating switch.

When measuring the distance from BCM to CO and from BCM to PBX systems, use 600 ohms as the termination resistance setting.

Table 12 Loss package settings

Loss Package	Receive Loss	Transmit Loss	Impedance	Distance to switch/cable loss/terminating switch
Short CO	0 dB	3 dB	Short	Short/<2 dB/BCM to CO
Medium CO	0 dB	0 dB	TIA/EIA 464	Medium/>2 dB and <6 dB/BCM to CO
Long CO	-3 dB	0 dB	TIA/EIA 464	Long/>6 dB/BCM to CO
Short PBX	0 dB	0 dB	Short	Short/<2 dB/BCM to PBX
Long PBX	-3 dB	0 dB	TIA/EIA 464	Long/>2 dB/BCM to PBX

A loss of 4 dB corresponds to a cable length of approximately 2700 m (9000 ft).

Note: Loss packages are not supported on the 4X16 combo.

Turn Privacy on or off for a call

You can configure lines in your system to have automatic privacy. With a line not programmed with privacy, anyone with the line assigned to their telephone can join your call by pressing the line button. With a line programmed with privacy, one person at a time can use the line.

Use **FEATURE 83** to turn the Privacy feature off and on.

Privacy control cannot be used for internal or conference calls.

When another telephone joins a call, the participants on the call hear a tone, and a message appears on the telephone display. It is not possible to join a call without everyone hearing this tone.

Note: The Auto privacy setting does not apply to target lines, PRI lines or VoIP trunking lines.

Programming line access

There are a number of ways you can configure your lines. You can assign each line to one telephone or several telephones, or a specific line to a specific telephone. You can also pool your lines so that a number of telephones have access to several lines.

See the following information:

- "Making lines available" on page 98
- "Incoming calls" on page 99
- "Outgoing calls" on page 99

Making lines available

- You can determine whether a line will be assigned solely to one telephone, or if a group of users will have access to the line.
- Even when you use line pools, it is possible that a line pool will be unavailable for outgoing traffic. To alleviate this, you can determine overflow paths for any routes that you designate.
- Incoming lines can be assigned to telephones as individual lines or through target lines, depending on the type of trunk supplied from the central office (CO). Incoming lines do not need to have an appearance on the telephone. Target lines are for incoming calls only. Two-way single lines, such as analog lines, allow the user to make an outgoing call by pressing the (idle) assigned line button or, if the line is part of a line pool, by entering a line pool access code or destination code to access the line pool. These lines can also be redirected on a per-trunk basis through Element Manager or from the telephone by using **FEATURE 84**.
- PRI lines are always configured into line pools. These lines require a destination code for outgoing calls. Incoming calls use target line assignments.

- Voice over IP (VoIP) trunks use the data network to provide line service in and out of the system. VoIP trunk configuration is described in the. VoIP trunks use target lines for incoming calls, and require line pool codes or destination codes for outgoing calls.
- You can assign a line a maximum of 93 times.

Incoming calls

For incoming calls, you can have a central answering position, or you can specify lines to one or more telephones to receive directed calling.

You can arrange your telephones in Hunt groups, ringing groups, or call groups that use system-wide call appearance (SWCA) assignments to share calls.

You can also configure lines for use by system users who call in from outside the system. You can give them direct access to the system with an Auto DN, or you can configure the line so they hear a stuttered dial tone, at which point they need to enter a password (CoS) to gain access (DISA DN).

Outgoing calls

For outgoing calls, you can assign one or more intercom keys to access a line pool or prime line, destination code, or internal system numbers to direct the call. Telephones without intercom keys do require intercom paths assigned, but to access calls, users must pick up the handset to connect.

For calls within the system, all telephones are virtually linked within the system. To call another telephone inside the system, you can lift the handset and dial the local DN. In this case, the prime line must be set to intercom.

For calls going outside the system:

- If you assign the prime line to a line pool — When you pick up the handset, the telephone automatically grabs the first available line from the assigned line pool. In this configuration, you must ensure that the outgoing number is allowed by the line pool.
- If you assign the prime line to an intercom button — You can enter a line pool access code or a destination code followed by the telephone number to direct the outgoing call where it exits the system on any available line in that pool.

Chapter 9
Configuring telephony resources

The Telephony Resources panel allows you to view and configure the information for the modules that support the digital/analog/ISDN lines for the system and the gateways that support the Voice over IP (VoIP) trunks. This provides a cohesive view of your telephony communications channels for the system.

The following paths indicate where to configure telephony resources in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Resources > Telephony Resources**
- Telset interface: ****CONFIG > Hardware** (you cannot configure VoIP trunks or IP telephones)

The following table provides links to descriptions of each subpanel.

Panel	Tasks
"Telephony Resources table" on page 102	"Managing modules" on page 87
"Media bay module panels" on page 104	"Configuring the trunk module parameters" on page 83
"Trunk Module Parameters" on page 104	
"Port details" on page 110	
"Call-by-Call Service Selection" on page 108	
Also refer to:	"Dialing plan: Private network settings" on page 281
	"Call security: Remote access packages" on page 439
"Provisioning module lines/loops" on page 112	
"IP telephones" on page 112	
"IP Terminal Global Settings" on page 113	"Registering Nortel IP telephones" in the *Telephony Device Installation Guide* (NN40020-309)
"IP telephone set details" on page 114	
"Voice over IP trunks" on page 115	
	"Configuring VoIP trunk gateways" on page 381
	"VoIP interoperability: Gatekeeper configuration" on page 389
"Routing table" on page 116	
"H323 Settings" on page 118	
"H323 Media Parameters" on page 122	"Setting up VoIP trunks for fallback" on page 391
"SIP Settings" on page 125	
"SIP Media Parameters" on page 126	
"SIP URI Map" on page 127	

Click the navigation tree heading to access general information about user management.

The top frame of this panel displays a table showing each type of module and the VoIP trunks that are assigned to the system, either through connections to a media bay module or by applying the required keycodes (VoIP trunks).

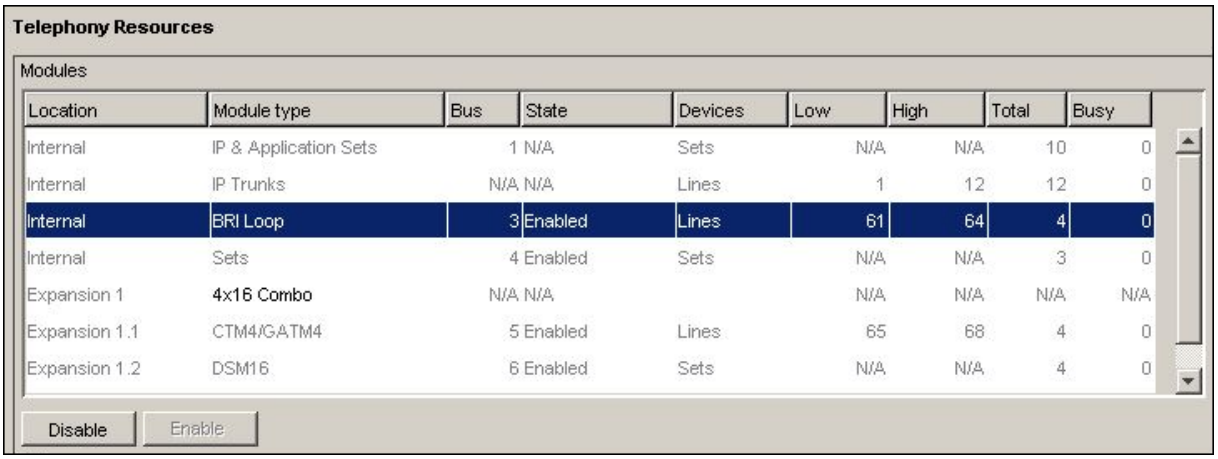
Selecting a table listing provides access to the special settings for each type of resource in tabbed panels that appear in the lower window.

Telephony Resources table

The top-level panel shows a list of active modules and VoIP gateways and IP telephone IP network information.

Click the line for the resource you want to view or configure.

Figure 22 Telephony Resources table


Telephony Resources
Modules
Location
Module type
Bus
State
Devices
Low
High
Total
Busy
Internal IP & Application Sets 1 N/A Sets N/A N/A 10 0
Internal IP Trunks N/A N/A Lines 1 12 12 0
Internal BRI Loop 3 Enabled Lines 61 64 4 0
Internal Sets 4 Enabled Sets N/A N/A 3 0
Expansion 1 4x16 Combo N/A N/A N/A N/A N/A N/A
Expansion 1.1 CTM4/GATM4 5 Enabled Lines 65 68 4 0
Expansion 1.2 DSM16 6 Enabled Sets N/A N/A 4 0
Disable
Enable

The Telephony Resources table fields are described in Table 13.

Table 13 Telephony Resources table fields (Sheet 1 of 2)

Attribute	Value	Description
Location	<read-only>	
Module type	<read-only> DID4 DID8 ASM/ASM+ GATM4 DSM16 DSM32/ DSM32+ 4X16 Combo 8X16 Combo DTM-T1 DTM-PRI CTM4/GATM4 CTM8/GATM8 BRIM Empty	This field indicates the type of module assigned to each location. DID4 DID8 ASM/GASM: Analog and Global Analog Station Modules provide four connections for four analog telephones. GATM8: Global Analog Trunk Module with four trunk line connections. DSM16 or DSM32/DSM32+: Digital Station Module with 16 and 32 telephone connections, respectively. 4X16 Combo: A module with 4 analog trunks and 16 digital stations. 8X16 Combo: A module with 8 analog trunks and 16 digital stations. BRI-ST DTM-T1 DTM-PRI Empty: No module is currently connected.
Bus	<read-only> 1-XX	This number indicates the virtual bus to which the module is assigned. For trunk modules, this position determines the default line numbers available to the trunks attached to the module. For station modules, this position determines the DN range that will automatically be assigned to telephones plugged into the module.
State	Enabled Disabled Unequipped	Indicates the state of the module or bus: Enabled: module is installed and working Disabled: module is installed but has been disabled or is down for another reason Unequipped: there is no module installed on this bus
Devices	Set Lines	Lists the type of device configured on the bus.
Low	<digits>	This field indicates the lowest setting for one of the following: The range of lines the module/VoIP supports The range of loops the module supports (BRI) The range of DNs the module/IP telephony supports.
High	<digits>	This field indicates the highest setting for one of the following: The range of lines the module/VoIP supports The range of loops the module supports (BRI) The range of DNs the module/IP telephony supports.
Total	<XX> Lines, loops or Sets	This field indicates the total number of lines, loops or DNs that the module supports.

Table 13 Telephony Resources table fields (Sheet 2 of 2)

Attribute	Value	Description
Busy	1-X	This field indicates the current activity for the devices or lines attached to the module.

Media bay module panels

The following panel tabs appear when you select a module table entry on the Telephony Resources panel.

- "Trunk Module Parameters"
- "Port details" on page 110

Note that the four trunks connected to the core module are also indicated in the table when they are active. These trunks are analog trunks.

Trunk Module Parameters

The Trunk Module Parameters tab shows the information that is unique to the type of trunk module selected in the main Modules list.

Figure 23 Trunk Module Parameters subpanel

Table 14 describes the possible fields, trunk module parameters, and an indication of which types of modules use each setting.

Table 14 Module parameters values (Sheet 1 of 4)

Attribute	Value	Module/line type
Trunk type		**All trunks**
	Indicates the type of trunks. This field is read-only for all modules except DTM modules.	
Trunk mode	DS/CLID, Global, Legacy	**Loop**

Table 14 Module parameters values (Sheet 2 of 4)

Attribute	Value	Module/line type
	• DS/CLID: displays for old North American LS/DS or CLID analog trunk modules, the old analog MBM, or the GATM with North American DIP switch settings. • Global: displays for the GATM MBM with no regional DIP switches set. • Legacy: displays for all other (old) analog trunk modules	
Protocol	NI-2, DMS-100, DMS-250, AT&T4ESS, SL-1, Euro, ETSI Q.Sig	**PRI**
	Choose the trunk protocol used by your service provider. The supported protocols are: **PRI-T1:** NI (NI-1 and NI-2), DMS-100, DMS-250, AT&T4ESS, SL-1 **PRI-E1:** ETSI QSIG, Euro, SL-1 **Note:** SL-1 and ETSI QSIG require an MCDN keycode to display. **BRI:** Protocol can also be selected on BRI T-loops under **Configuration > Telephony > Loops**. **Note:** Always check the line protocol with the central office.	
NSF Extension	None, WATS, ALL	**PRI**
	The Network Specific Facilities (NSF) information element is used to request a particular service from the network. Settings are based on the type of switch to which the line connects. Suggested settings: DMS-100/250: NONE Siemens ESWD, Lucent 5ESS: WATS GTD5, DMS-10: ALL When you select **NONE**, the NSF extension bit is not set for any service. When you select **WATS**, the NSF extension bit is set for unbanded OUTWATS calls. When you select **ALL**, the NSF extension is always set for all CbC services. Appears only for NI protocol.	
Protocol type	User, Network	**PRI**
	When you select SL-1 protocol, an additional setting, Protocol type, appears. SL-1 protocol is a private networking protocol. Use this protocol to designate a BCM node as a Network (controller). The default setting is User (client). In public network configurations, the CO is generally considered the Network side or controller. Applies to SL-1 protocol only.	
B-channel selection sequence	Ascending Sequential Descending Sequential	**PRI**
	Defines how B-channel resources are selected for call processing.	
Answer timer	1, 2, 3, 4, or 5 sec.	E&M PRI
	Set the minimum duration of an answer signal before a call is considered to be answered.	

Table 14 Module parameters values (Sheet 3 of 4)

Attribute	Value	Module/line type
Disconnect timer	60, 100, 260, 460, or 600 milliseconds	Loop T1
	Specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO). You must enable disconnect supervision by changing the Line **Trunk mode** attribute. Under the Telephony Services sub-heading, choose Lines and Line/trunk Data.	
Clock Source	Primary External Secondary External Internal	T1 PRI *BRI S/T **DASS2**
	Designates whether the DTM/BRI acts as a primary or secondary timing component for an external timing source or as the internal timing source. **Note:** A BRI module can be programmed with primary/secondary clock source, however, it is recommended that a BRI module always be set to Internal if a DTM exists on the system to be the Primary External clock source. **Warning: Changing the clock source may disconnect calls**. If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.	
Send Name Display	Select or clear	PRI *BRI QSIG
	When you select this check box, the system sends a specified outgoing name display (OLI) from the calling telephone. Appears only for Protocols: SL-1, NI, DMS-100, DMS-250, or PRI QSIG.	
Remote Capability MWI	Select or clear	PRI
	Use this setting to indicate MWI compatibility on the specific loop(s) that you are using to connect to the central voice mail system on a Meridian 1, that has the MWI package installed, with the RCAP setting set to MWI. Appears only for SL-1 protocol.	
Host node	M1, Embark, IDPX, DSM	DNPSS
	DPNSS cards connected to Embark switches have a different way of handling call diversion, therefore, when you provision a DTM for DPNSS, you must indicate what type of switch the lines are connected to. When you select the Embark switch, calls are diverted using the Call Forwarding feature instead of call diversion.	
Local Number Length		DPNSS
	This number allows the system to determine how many digits to read on an incoming call to determine that the call is meant for this system.	
Maximum Transits	Default: 31	PRI
	Indicate the maximum number of times that a call will be transferred within the SL-1 network before the call is dropped. Protocol must be set to SL-1 to display this field.	

Table 14 Module parameters values (Sheet 4 of 4)

Attribute	Value	Module/line type
T1 parameters		
CO fail		**T1** **PRI**
	Specify a carrier failure standard (T1A-5474, TR62411)	
Interface levels	ISDN, PSTN	**T1** **PRI**
	Define a loss plan setting. For more information, see "Interface levels" on page 107.	
Framing	ESF, SF	**T1** **PRI**
	Select the framing format used by your T1 or PRI service provider: Extended Superframe (ESF) or Superframe (SF). Contact your T1 or PRI service provider for the proper setting. (SF or Superframe is sometimes known as D4.)	
Line coding	B8ZS, AMI	**T1** **PRI**
	Define the encoding signals on a T1 line. Select the standard used by your T1 service provider. Contact your T1 service provider for the proper setting.	
Internal CSU	<check box>	**T1** **PRI**
	Turn the internal T1 channel service unit (CSU) on or off. For more information, see "Internal CSU" on page 108.	
CSU line build	0, 7.5, or 15 dB	**T1** **PRI**
	Set the gain level of the transmitted signal. This setting appears only when the Internal CSU is Enabled.	
DSX1 build	000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet	**T1** **PRI**
	Set the distance between BCM and an external channel service unit. This setting appears only when the Internal CSU is Disabled. Contact your service provider for the proper settings.	
CRC4	<check box>	**E1** **PRI**
	Ensure this is enabled or disabled to match the service provider Cyclic Redundancy Check (CRC4) setting for the trunk.	

Station modules do not have any configurable module parameters.

Interface levels

The default Interface levels are the ISDN loss plan settings. Also refer to "ISDN overview" on page 535.

Check with your telecommunications service provider to determine if your BCM system is connected to a central office (CO) with digital network loss treatment (ISDN I/F levels) or analog network loss treatment (PSTN I/F levels).

The ISDN setting requires digital access lines (DAL) that have digital network loss treatment. On a DAL network, the PBX system administers the dB loss, not the CO. DALs may have ISDN signaling or digital signaling (for example, T1). The loss plan follows the Draft TIA-464-C loss plan, which uses a send loudness rating (SLR) of 8 dB. You must contact your service provider to get DAL network loss treatment on a line with digital signaling.

The PSTN setting requires analog access lines (AAL) that have analog network loss treatment and digital signaling. On an AAL(D) network, the CO administers the dB loss.

The loss plan follows the Draft TIA-464-C loss plan. The ISDN loss plan uses a send loudness rating (SLR) of 8 dB and a receive loudness rating (RLR) of 2 dB. The PSTN loss plan uses an SLR of 11 dB and an RLR of -3 dB. If you choose the wrong setting, the voice signal can be too loud or too soft.

Internal CSU

Internal CSU allows you to turn the internal T1 channel service unit on or off. The channel service unit gathers performance statistics for your T1 lines or PRI with public interface. Contact your service provider for the correct settings.

You can view the performance statistics for your T1 lines in Maintenance under the CSU stats heading. Before you set the internal CSU to off, you must ensure there is an external CSU connected to your T1 lines.

Call-by-Call Service Selection

This following provides information about how to configure the PRI Call-by-call Service Selection, which is region-specific to North America, for a DTM set to a PRI Module type.

By default, incoming calls on a PRI are routed based on the Called Party Number information within the call request. The last number of digits of the called party number that match the Received Number Length setting are used as Receive Digits to find a target line.

In North American PRI, the Call-by-Call services allows alternate routing maps to be defined in various ways, depending on the protocol defined for this PRI.

Figure 24 Call-by-Call Service Selection subpanel

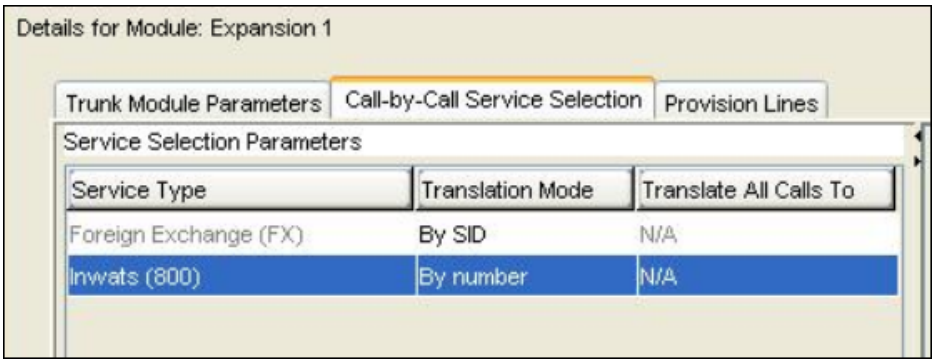


Table 15 describes the fields shown on the Call-by-Call Service Selection tab panel.

Table 15 Call-by-Call Service selection panel fields

Attribute	Value	Description
Service Type	Foreign Exchange Inwats (1-800) Intl-800 Digital (SDS) 900	Refer to "CbC services available by switch protocol" on page 110.
Translation Mode	None All By SID By Number	Define how the incoming digits get mapped to line numbers (target lines or DISA/AUTO DNs) within the system.
Translate All Calls To		Enter the appropriate information for the mode chosen.
Actions		
Add	1. On the Modules table, select the PRI module you want to configure. 2. Select the Service Type record to which you want to add Digit translations 3. Under the Translate table, click **Add**. 4. Enter the appropriate information in the From and To fields on the dialog box. 5. Click **OK** on the dialog to save the translation range.	
Delete	1. On the Modules table, select the PRI module record you want to delete. 2. Select the Service Type record from which you want to delete Digit translations 3. On the Translate table, select one or more ranges to delete. 4. Click **Delete**. 5. Click **OK** on the confirmation dialog to delete the digit translation range.	

CbC services available by switch protocol

Table 16 lists the applicable services for the protocol defined on the Module record.

Table 16 Services available for each PRI protocol

Protocol	Services Available				
	Foreign Exchg	**Inwats (800)**	**Intl-800**	**Switched Digital (SDS)**	**Nine Hundred (900)**
NI	SID or All	By number or All	N/A	N/A	N/A
DMS-100	SID or All	SID, By number, or All	N/A	N/A	N/A
DMS-250	SID or All	SID, By number, or All	N/A	N/A	SID, or By number, or All
4ESS	N/A	By number or All	By number or All	By number or All	By number or All

Port details

Both trunk and analog modules show port details. Ports settings are directly related to the physical ports into which the PSTN lines or telephony devices connect on the media bay modules.

The station module Port Details panel is illustrated in Figure 25. The trunk module Port Details panel is illustrated in Figure 26.

Figure 25 Station module Port Details panel

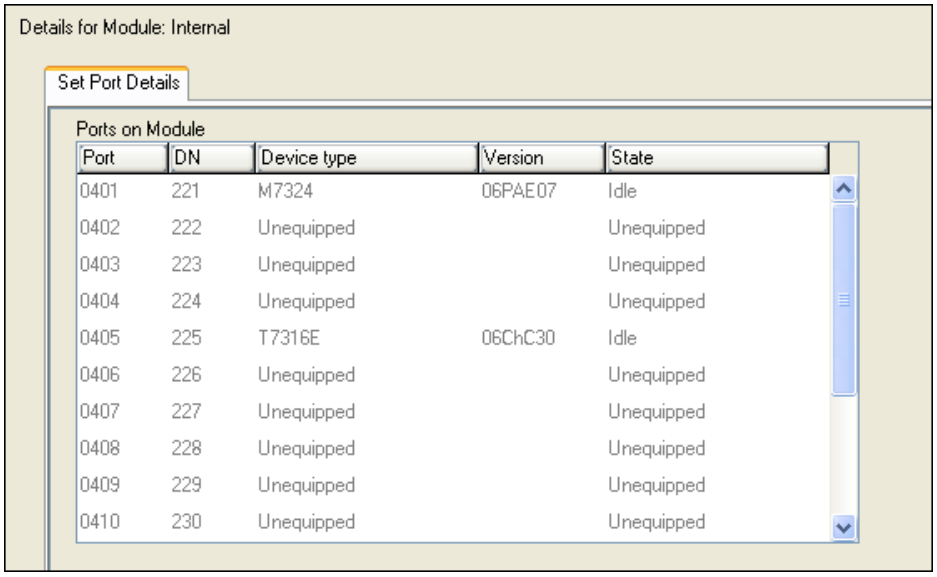


Figure 26 Trunk module Port Details panel.

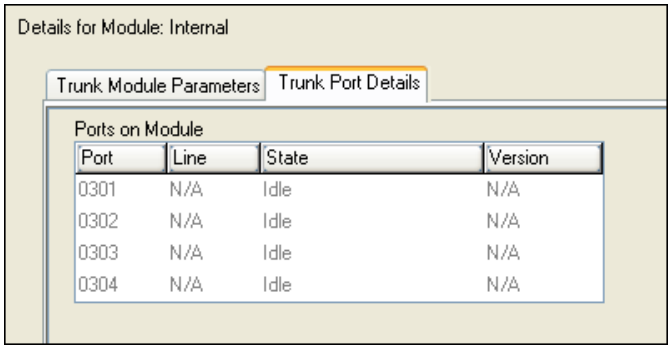


Table 17 describes the fields shown on the Port Values tab panel.

Table 17 Port Values tab

Attribute	Value	Module type
Port #	Read-only	**All modules**
	• These are the port numbers of the physical device.	
Device type	Read-only	**All modules**
	• This is the type of module.	
Line #	00X-XXX	**CTM/ GATM4** | **CTM/ GATM8** | **Combo** | **DTM-T1** | **DTM-PRI** | **BRI-T**
	The number of lines depends on the module type.	
Call State or State	Idle Active Deprovisioned	**All modules**
	This field indicates whether a module line or DN is in use or even provisioned.	
Version	<read-only>	**All modules**
	This field indicates the version of firmware running on the module.	
DN	XXXX	**ASM/ GASM** | **DSM**
	Each port supports one telephone, hence, one DN record.	
Addons		**All modules**
	Indicates auxiliary items added to the telephony devices or trunks	
	Add-on	This is a list number.
	Type	This field indicates the type of add-on, such as a KIM module.
	Version	This field indicates the version of firmware running on the add-on device.

Provisioning module lines/loops

You can access three provisioning subpanels in Element Manager at by clicking **Configuration > Resources > Telephony Resources**. The tabbed provisioning panel that appears depends on the type of module that is selected on the Telephony Resources table.

The provisioning subpanels are as follows:

- The Provision Line tab panel is used for all trunks except DPNSS and BRI loops.
- The DPNSS module displays the Provision Virtual Channels tab panel.
- BRI loops require an extra step, so the Provision Loops tab panel appears when a BRI module is selected.

Table 18 describes the fields on these panels.

Table 18 Provisioning panels

Field	Value	Description
Provision Lines tab		
Line	<line number>	This is a list of the lines assigned to the module.
Provisioned	<check box>	If the check box is selected beside a line, that line is available for call traffic.
Provision Virtual Channels tab		
Virtual Channel	<read-only>	A virtual channel assigned to the DPNSS module.
Provisioned	<check box>	If the check box is selected beside a channel, that channel is available for call traffic.
Provision Loops tab		
Loop	<loop-number>	These are the loop numbers assigned to the selected BRI module. Modules have four loops, but only loops designated as T-loops require provisioning.
Provisioned	<check box>	If the check box is selected beside a loop, that loop has lines that can be provisioned.
Line	<line number>	Each loop as two lines assigned. You can provision or deprovision these lines individually.
Provisioned	<check box>	If the check box is selected beside a line, that line is available for call traffic.

IP telephones

The following tabbed panels appear when you select an IP terminals entry on the Telephony Resources table.

- "IP Terminal Global Settings"
- "IP telephone set details" on page 114

IP Terminal Global Settings

The parameters on the IP Terminal Global Settings subpanel affect all Nortel 1120/1140/20XX IP telephones. This is also the panel you use to allow these telephones to register to the system, and to turn off registration once you have registered all the telephones.

Figure 27 IP Terminal Global Settings subpanel

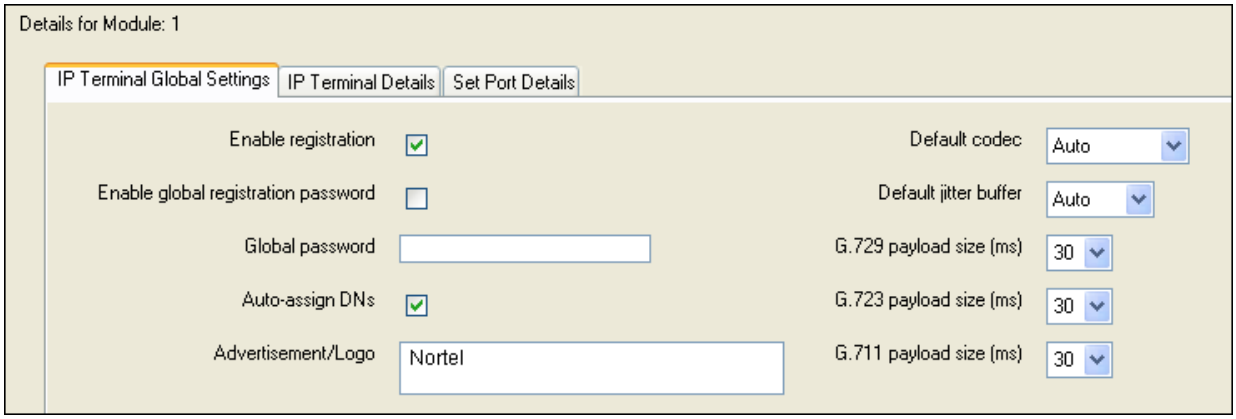


Table 19 defines the fields on this panel and indicates the lines.

Table 19 IP terminal Global panel fields (Sheet 1 of 2)

Field	Value	Description
Enable registration	<check box>	Select this check box to allow new IP clients to register with the system. **Warning:** Remember to clear this check box when you finish registering the new telephones.
Enable global registration password	<check box>	If selected, the installer will be prompted for the global registration password when registering a new IP client. If cleared, the installer will be prompted for a user ID and password combination that has “Installer” privileges. See the *Administration Guide* (NN40020-600) for information on accounts and privileges.
Global password	<10 alphanumeric> Default: bcmi (2264)	If the Enable global registration password check box is selected, enter the password the installer will enter on the IP telephone to connect to the system. If this field is left blank, no password prompt occurs during registration.
Auto Assign DN	<check box>	If selected, the system assigns an available DN as an IP terminal requests registration. It does not prompt the installer to enter a set DN. **Note:** For this feature to work, **Registration** must be selected. If not selected, the installer receives a prompt to enter the assigned DN during the programming session.
Advertisement/Logo	<alphanumeric string>	Any information in this field appears on the display of all IP telephones. For example, your company name or slogan.

Table 19 IP terminal Global panel fields (Sheet 2 of 2)

Field	Value	Description
Default Codec	Auto G.711-aLaw G.711-uLaw G.729 G723 G.729 + VAD G.723 + VAD	If the IP telephone has not been configured with a preferred codec, choose a specific codec that the IP telephone will use when it connects to the system. If you choose **Auto**, the system will select the most appropriate Codec when the IP telephone is on a call. If you are unsure about applying a specific codec, ask your network administrator for guidance.
Default jitter buffer	None Auto Small Medium Large	Choose one of these settings to change the default jitter buffer size: None: Minimal latency, best for short-haul networks with good bandwidth. Auto: The system dynamically adjusts the size. Small: The system adjusts the buffer size, depending on CODEC type and number of frames per packet to introduce a 60-millisecond delay. Medium: 120-millisecond delay Large: 180-millisecond delay
G.729 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 30	Set the maximum required payload size, per codec, for the IP telephone calls sent over H.323 trunks. **Note:** Payload size can also be set for Nortel IP trunks. Refer to "Configuring VoIP trunk media parameters" on page 382.
G.723 payload size (ms)	30	
G.711 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 20	

IP telephone set details

After a Nortel 1120/1140 or 20XX IP telephone registers with the system, this panel displays the terminal parameters.

The telephone is identified to the system by its IP address, so this cannot be changed. If you need to change the IP address of a telephone, you need to deregister the telephone and then register it again with the new IP address.

Figure 28 IP Terminal Details (Telephony Resources) subpanel

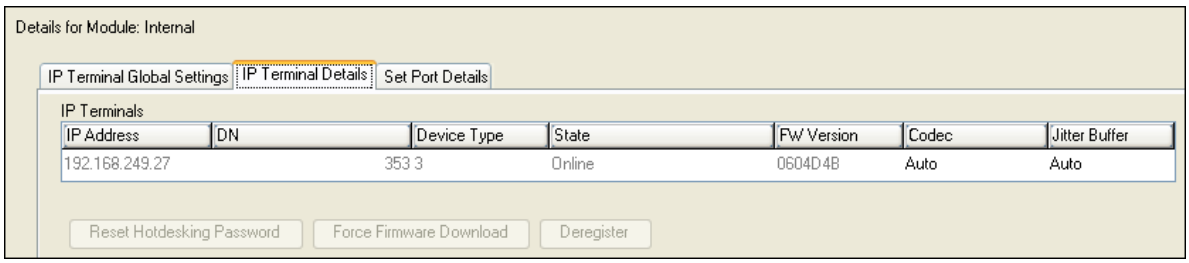


Table 20 describes the fields on this panel.

Table 20 IP terminal fields

Field	Value	Description
IP Address	<read-only>	If the telephone is using DHCP or partial DHCP, this may vary.
DN	<DN>	This is the DN record that defines the system parameters for the telephone.
Device Type	<read-only>	This is the type of IP telephone.
State	<read-only>	Indicates if the device is online,
FW Version	<read-only>	Current version of telephone software.
Codec	Default G.711-aLaw G.711-uLaw G.711 + VAD G.729 G.729 + VAD G.723	Specifying a non-default Codec for a telephone allows you to override the general setting. You might, for example, want to specify a low bandwidth Codec (G.729) for a telephone that is on a remote or busy sub-net. **Note:** You can change the codec on a configured IP telephone only if it is online to the system, or if Keep DN Alive is enabled for an offline telephone.
Jitter Buffer	Auto Default None Small Medium Large	Increase the jitter buffer size for any telephone that has poor network connectivity to the system. **Note:** You can only change the jitter buffer on a configured IP telephone if it is online to the system, or if Keep DN Alive is enabled for an offline telephone.
Actions		
Reset Hotdesking password	Click this button to reset the hotdesking password for a telephone. See the *Device Configuration Guide* (NN40020-300).	
Force Firmware Download	This button downloads the firmware from the system to the selected telephone. See the *Device Configuration Guide* (NN40020-300).	
Deregister	Click this button to deregister the selected telephone. See the *Device Configuration Guide* (NN40020-300).	

Voice over IP trunks

The following tabbed panels appear when you select a VoIP trunk entry on the Telephony Resources panel. See the following topics for a description of each tabbed panel and their fields.

- "Routing table" on page 116
- "H323 Settings" on page 118
- "H323 Media Parameters" on page 122

- "SIP Settings" on page 125
- "SIP Media Parameters" on page 126
- "SIP URI Map" on page 127

Routing table

Both H.323 and SIP trunks are automatically assigned to line pool BlocA. The decision about whether a given call is through SIP or H.323 is made from the information in the Routing Table. Calls can be routed directly from entries in the Routing Table, or can use the services of a redirect proxy or gatekeeper.

Note: If BCM has keycodes for H323 and SIP, check the BCM DNS configuration to prevent issues in enabling VoIP trunks in H323 or SIP protocols.

Figure 29 Routing Table

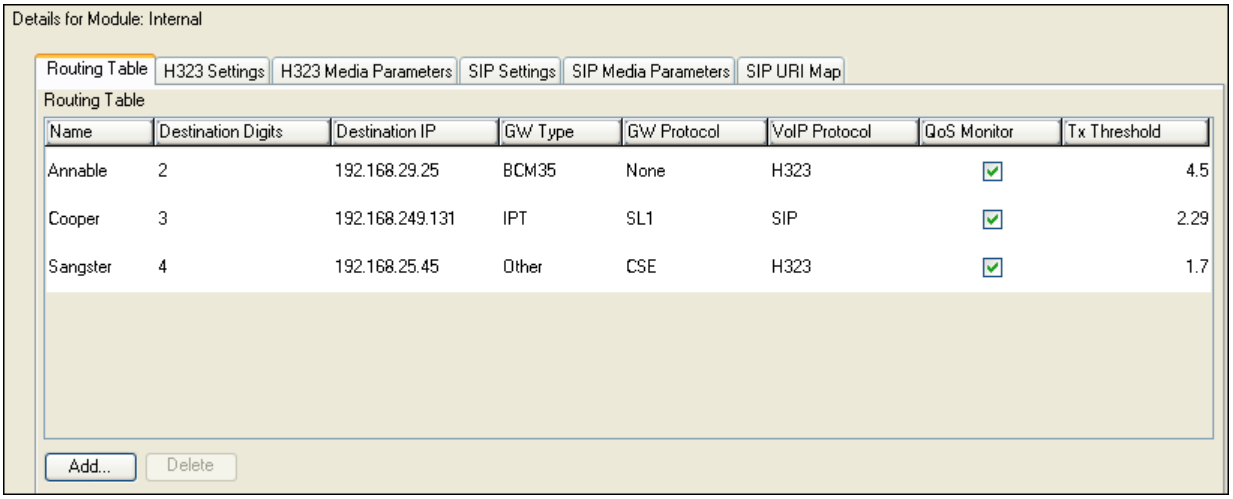


Table 21 Routing Table fields (Sheet 1 of 2)

Attribute	Value	Description
Name	<alphanumeric>	Enter the name of the remote system
Destination Digits	<numeric> (could be the same as the destination code for the route to this system)	Set the leading digits which callers can dial to route calls through the remote gateway. Ensure that there are no other remote gateways currently using this combination of destination digits. If multiple leading digits map to the same remote gateway, separate them with a space. For example, 7 81 9555. These numbers are passed to the remote system as part of the dialed number.
Destination IP	<IP Address>	Enter the IP address of the remote system gateway.

Table 21 Routing Table fields (Sheet 2 of 2)

Attribute	Value	Description
GW Type	BCM BCM35 IPT Other	Choose the type of system that is accessed through the remote gateway: BCM: BCMs running 3.6 or later software and CallPilot with compatible versions of H.323. BCM35: for BCMs running 3.5 software. IPT: Meridian 1 system running IP software.
GW Protocol	SL1 CSE None	Select the gateway protocol that the trunk expects to use. None: No special features. SL1: Use for BCM 2.5 systems only that require MCDN over VoIP trunks. CSE: MCDN protocol for gateways that provide VoIP service through Meridian 1 IPT (BCM 3.6 and newer software) or CSE1000 gateways (BCM 3.0 and newer software)
VoIP Protocol	H323 SIP	Select the routing protocol for your network.
QoS Monitor	<check box>	If you intend to use a fallback PSTN line for this gateway, ensure that this check box is selected. Ensure that QoS Monitor is also enabled on the remote system. Otherwise, leave the check box empty.
Tx Threshold	<0-5>	Indicate the level of transmission at which the signal must be maintained. If the signal falls below this level the call falls back to PSTN. Default: 0
Actions		
Add	1. On the Remote Gateways panel, click **Add**. 2. On the **Add** dialog: 3. **Name:** Enter a short descriptive title for the remote system. 4. **Destination IP**: Enter the public IP address of the remote system. 5. Click **OK**. 6. On the Remote Gateways panel, click in the fields to set any other parameters that you require.	
Delete	1. On the Remote Gateways panel, select the gateway you want to delete. 2. Click **Delete**. 3. Click **OK** on the confirmation dialog box.	

H323 Settings

Figure 30 H323 Settings

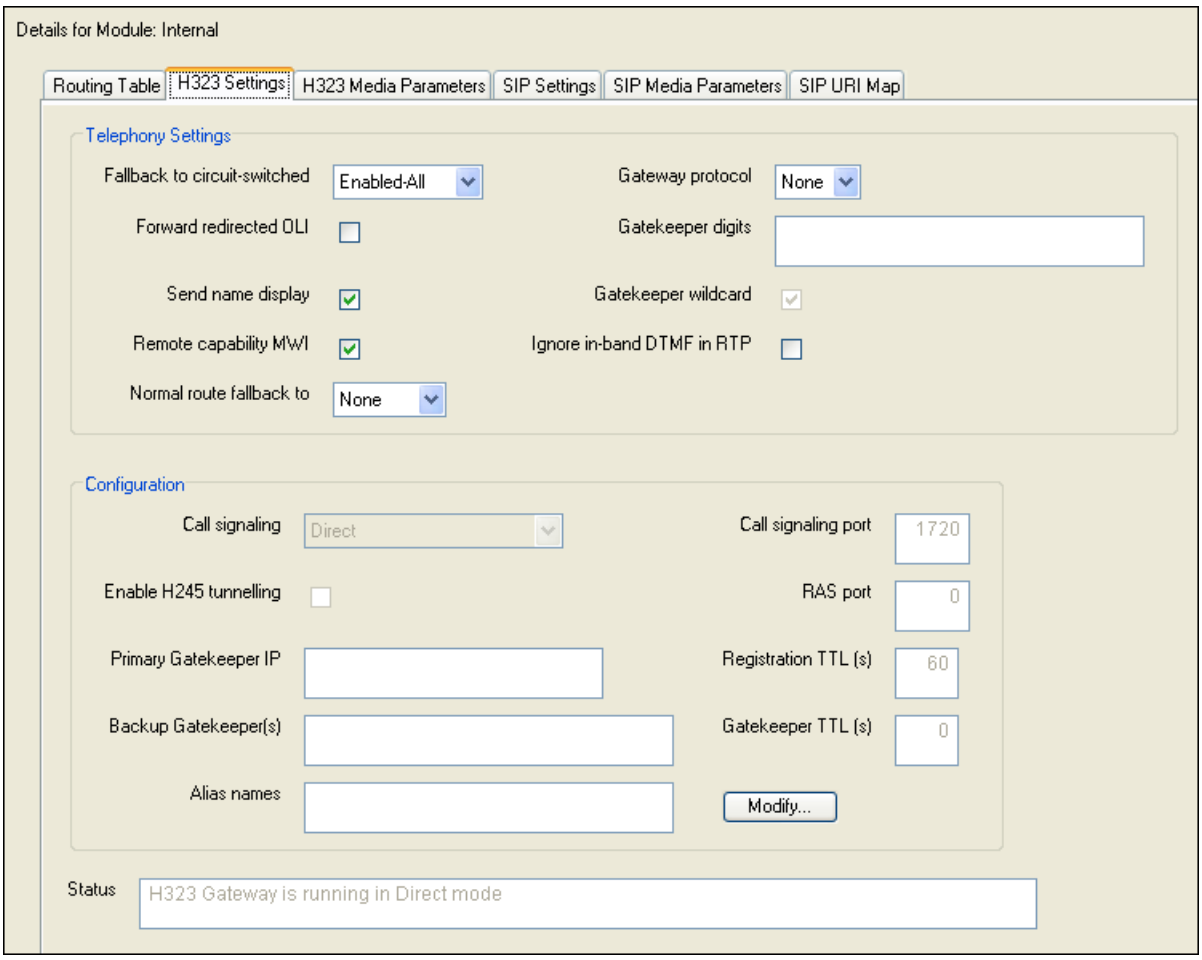


Table 22 describes the fields on the H323 Settings tab.

Table 22 H323 Settings fields (Sheet 1 of 5)

Field	Value	Description
Telephony Settings		
Fallback to circuit-switched	Enabled-All Enabled-TDM Disabled	Your choice determines how the system will handle calls if the IP network cannot be used. • Enabled-All: All calls are rerouted over specified PSTN trunks lines. • Enabled-TDM: All TDM (digital telephones) voice calls will be rerouted over specified PSTN trunks lines. • Disabled: Calls will not be rerouted.
	Note: Enabled-TDM-only enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because PSTN fallback is unlikely to result in better quality of service in that scenario.	

Table 22 H323 Settings fields (Sheet 2 of 5)

Field	Value	Description
Forward redirected OLI	<check box>	If the check box is selected, the OLI of an internal telephone is forwarded over the VoIP trunk when a call is transferred to an external number over the private VoIP network. If the check box is cleared, only the CLID of the transferred call is forwarded.
Send name display	<check box>	When selected, the telephone name is sent with outgoing calls to the network.
Remote capability MWI	<check box>	This setting must coordinate with the functionality of the remote system hosting the remote voice mail.
Normal route fallback to	None Prime set	Select None or Prime set. If Prime set is selected and the outgoing IP trunk leg of the call in a tandem scenario cannot be completed, the call will terminate on the prime set for the line. Default: None
Gateway protocol	None SL1 CSE	Both these protocols require a keycode. SL1: Use this protocol only for BCM 2.5 systems CSE: Use this protocol for BCM 3.0 and later systems. This protocol supports Meridian 1 IPT. Otherwise, use None.
Gatekeeper digits	<0-9>	If dialed digits match gatekeeper digits, the call is routed via H323 protocol. If the digits do not match, the call is routed via SIP protocol.
Gatekeeper wildcard	<check box>	If selected, all dialed digits match gatekeeper digits and VoIP calls will be routed through the gatekeeper.
Ignore in-band DTMF in RTP	<check box>	If selected, the BCM ignores audible in-band DTMF tones received over VoIP trunks after the BCM connects the remote end to a locally hosted call center application, or a locally hosted CallPilot application such as auto attendant, voice mail or IVR. **Note**: This setting is useful (should be selected) when the far end is a Call Server 2000 (CS2K) & Packet Voice Gateway (PVG) combination where the PVG is provisioned for OOBDTMFSupp=FullSupport resulting in the PVG + CS2K sending out-of-band, as well as in-band, DTMF tones at the same time to the BCM. The PVG MAY not send both tone notifications depending on whether the call is using G711 and the version of the CS2K software release (i.e. SNxx). This setting should be co-coordinated with the CS2K administrator. Default: Cleared

Table 22 H323 Settings fields (Sheet 3 of 5)

Field	Value	Description
Configuration		
*Call signaling	Direct Gatekeeper Resolved Gatekeeper Routed Gatekeeper Routed no RAS	Direct: call signaling information is passed directly between endpoints. The remote gateway table in the Element Manager defines a destination code (digits) for each remote system to direct the calls for that system to route. In each system, the Nortel IP Terminals and H.323 Terminals records map IP addresses to specific telephones. Gatekeeper Resolved: all call signaling occurs directly between H.323 endpoints. This means that the gatekeeper resolves the phone numbers into IP addresses, but the gatekeeper is not involved in call signaling. Gatekeeper Routed: uses a gatekeeper for call setup and control. In this method, call signaling is directed through the gatekeeper. Gatekeeper Routed no RAS: Use this setting for a NetCentrex gatekeeper. With this setting, the system routes all calls through the gatekeeper but does not use any of the gatekeeper Registration and Admission Services (RAS).
Enable H245 tunneling	<check box>	If Enabled, the VoIP Gateway tunnels H.245 messages within H.225. The VoIP Gateway service must be restarted for a change to take effect. Default: Disabled.
Primary Gatekeeper IP	<IP address>	If Gatekeeper Routed, Gatekeeper Resolved or Gatekeeper Routed no RAS are selected under Call Signaling, type the IP address of the machine that is running the gatekeeper.
Backup Gatekeeper(s)	<IP address> <IP address>	NetCentrex gatekeeper does not support RAS; therefore, any backup gatekeepers must be entered in this field. **Note:** Gatekeepers that use RAS can provide a list of backup gatekeepers for the end point to use in the event of the primary gatekeeper failure.

Table 22 H323 Settings fields (Sheet 4 of 5)

Field	Value	Description
Alias Names	Alias names are comma delimited, and may be one of the following types: **E.164** — numeric identifier containing a digit in the range 0-9. Identified by the keyword `TEL:` Example: the BCM is assigned an E.164 and an H323 Identifier: `Alias Names: TEL:76, NAME:bcm10.nortel.com` • NPI-TON — also referred to as a PartyNumber alias. Similar to E164 except that the keyword indicates the NPI (numbering plan identification), as well as the TON (type of number). Identified by one of the following keywords: `PUB` (Public Unknown Number); `PRI` (Private Unknown Number); `UDP` (Private Level 1 Regional Number (UDP)); `CDP` (Private Local Number (CDP)).	
	• H.323Identifier — alphanumeric strings representing names, e-mail addresses, etc. Identified by the keyword `NAME:` Example: The BCM is assigned a public dialed number prefix of 76, a private CDP number of 45, and an H323 Identifier alias: `Alias Names: PUB:76, CDP:45, NAME:bcm10.nortel.com`	
	• H.225 (Q.931) CallingPartyNumber (NetCentrex gatekeeper) — The NetCentrex gatekeeper uses the H.225(Q.931) CallingPartyNumber to resolve the call originator for billing purposes. This number must then contain a unique prefix, or location code that is unique across all endpoints that are using the NetCentrex gatekeeper. Identified by the keyword **`src:`**. Example for private networks: CDP alias = src:<DN>; UDP alias = src:<LOC><DN>. Example for public network: src:<public OLI>	
	Note: E164 or NPI-TON alias types are commonly used since they fit into dialing plans. A BCM alias list should not mix these types. Also, the type of alias used should be consistent with the dialing plan configuration. Use the same alias naming method on all BCMs within a network.	
Configuration note:	Refer to "Using CS 1000 as a gatekeeper" on page 389 for specific information about configuring the gatekeeper for H.323 trunks.Network note: If your private network contains a Meridian 1-IPT, you cannot use Radvision for a gatekeeper.	
If Gatekeeper Routed, Gatekeeper Resolved, or Gatekeeper Routed no RAS are selected under Call Signaling, enter one or more alias names for the gateway.		
Call signaling port	0-65535	Default: 1720 This field allows you to set non-standard call signaling port for VoIP applications that require special ports. 0 = The first available port is used. Ensure that you do not select a port that has been assigned elsewhere in the BCM. To ensure the port is not in use, run netstat-a from the command line.
RAS port	0-65535	Default: 0 This field allows you to set a non-standard Registration and Admission (RAS) port for VoIP applications that require special ports. 0 = The first available port is used. Ensure that you do not select a port that has been assigned elsewhere in the BCM. To ensure the port is not in use, run netstat-a from the command line.
Registration TTL (s)	Default: 60 seconds	This TimeToLive parameter specifies the intervals when the VoIP gateway sends KeepAlive signals to the gatekeeper. The gatekeeper can override this timer and send its own TimeToLive period.

Table 22 H323 Settings fields (Sheet 5 of 5)

Field	Value	Description
Gatekeeper TTL (s)		The actual time used by the gatekeeper for the registration process.
Status	<read-only>	Indicates if the device is online.
Modify	<button>	Click to modify the parameters. **Note**: All active H.323 calls are dropped if these settings are changed.

H323 Media Parameters

The H323 Media Parameters tab defines how VoIP trunks handle the signals. This panel also includes the settings to enable T.38 Fax signals over the trunks.

Figure 31 H323 Media Parameters panel

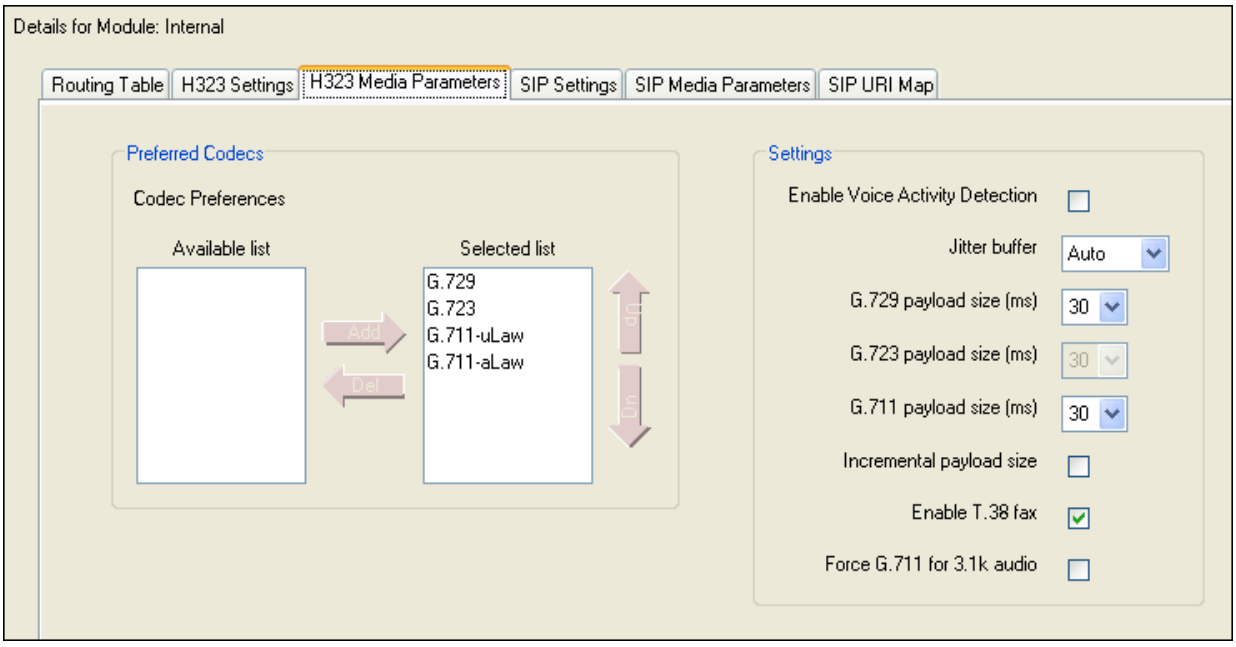


Table 23 describes the fields on this panel.

Table 23 H323 Media parameters record (Sheet 1 of 2)

Field	Value	Description
Preferred Codecs		
Preferred Codecs	None G.711-uLaw G.711-aLaw G.729 G.723	Select the Codecs in the order in which you want the system to attempt to use them. **Performance note:** Codecs on all networked BCMs must be consistent to ensure that interacting features such as Transfer and Conference work correctly. Systems running BCM 3.5 or later software allow codec negotiation and renegotiation to accommodate inconsistencies in Codec settings over VoIP trunks. **Note**: The G.723 codec can be used between IP endpoints. If other types of connections are required, ensure one of the other codecs is also selected.
Actions		
	1. On the Available list, click the codec you want to add to the Selected list. 2. Click the button to move the codec to the Selected list.	
	1. Select a codec that you want to remove from the Selected list. 2. Click this button to move the codec back to the Available list.	
	1. Select a codec on the Selected list. 2. Click the appropriate arrow to move the codec up or down in the Selected list.	

Table 23 H323 Media parameters record (Sheet 2 of 2)

Field	Value	Description
Settings		
Enable Voice Activity Detection	<check box>	The voice activity detection, also known as silence suppression identifies periods of silence in a conversation, and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. For more information refer to "Silence suppression" on page 529. If voice activity detection is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support voice activity detection. G.711 does not support voice activity detection. **Performance note:** Voice activity detection on all networked BCMs and IPT systems (VAD setting on IPT systems) must be consistent to ensure that interacting features such as Transfer and Conference work correctly. As well, the Payload size on the IPT must be set to 30ms. Default: Disabled
Jitter buffer	Auto None Small Medium Large	Select the size of jitter buffer you want to allow for your system. Default: Auto
G.729 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 30	Set the maximum required payload size, per codec, for the VoIP calls sent over H.323 trunks. **Note:** Payload size can also be set for Nortel IP telephones. See the *BCM 4.0 Telephony Device Installation Guide (N0027269)*.
G.723 payload size (ms)	30	
G.711 payload size (ms)	10, 20, 30, 40, 50, 60 Default: 30	
Incremental payload size	<check box>	When enabled, the system advertises a variable payload size (40, 30, 20, 10 ms)
Enable T.38 fax	<check box>	Enabled: The system supports T.38 fax over IP. Disabled: The system does not support T.38 fax over IP
		Caution: Operations note: Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference: Locate fax machine away from other telephones. Turn the speaker volume on the fax machine to the lowest level, or off, if that option is available.
Force G.711 for 3.1k Audio	<check box>	When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals such as modem or TTY machines. **Note**: This setting can also be used for fax machines if T.38 fax is not enabled on the trunk.

SIP Settings

Figure 32 SIP Settings tab

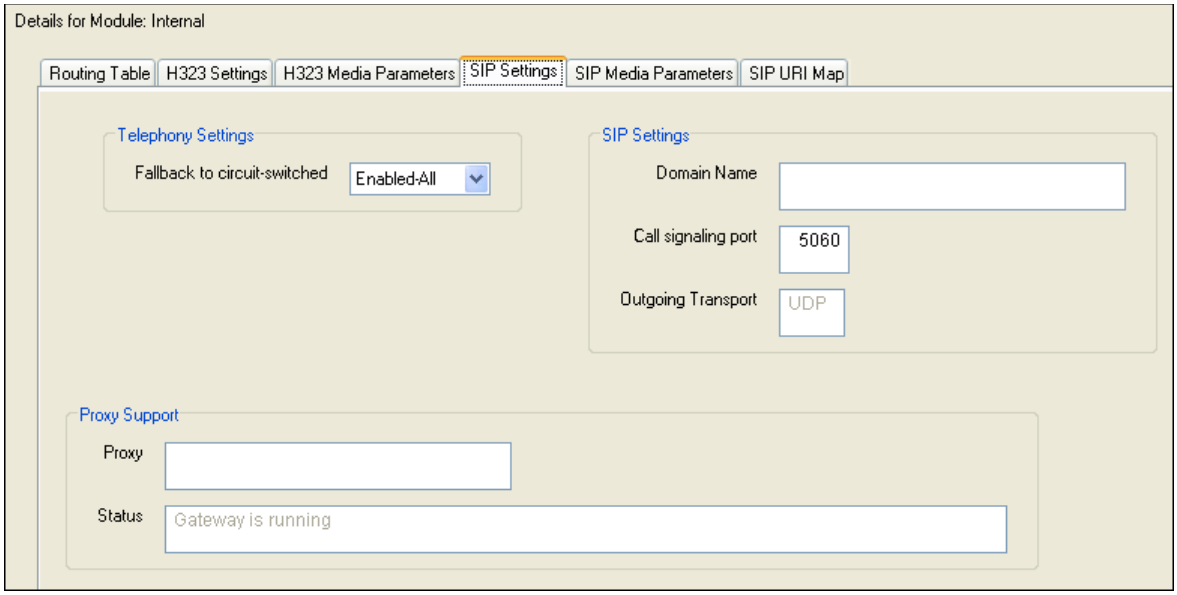


Table 24 SIP Settings fields

Field	Value	Description
Telephony Settings		
Fallback to circuit-switched	Enabled-All Enabled-TDM Disabled	Your choice determines how the system will handle calls if the IP network cannot be used. • Enabled-All: All calls will be rerouted over specified PSTN trunks lines. • Enabled-TDM: All TDM (digital telephones) voice calls will be rerouted over specified PSTN trunks lines. • Disabled: Calls will not be rerouted. Default: Enabled-All
SIP Settings		
Domain Name		Domain of the SIP network.
Call signaling port		This is the listening port for the BCM **Note**: FEPS (Functional Endpoint Proxy Server) must be restarted if this values is changed. Default: 5060
Outgoing Transport	UDP	The outgoing transport protocol for the gateway. **Note**: UDP is the only transport supported by the SIP enabled data services. Default: UDP
Proxy Support		
Proxy	<IP address>	Specify the IP address of the SIP proxy server.
Status	<read-only>	Indicates the status of the gateway.

SIP Media Parameters

SIP trunks are administered separately from H.323 trunks. Both H.323 and SIP trunks commonly h exist on the same system; however, each has different network settings.

Figure 33 SIP Media Parameters tab

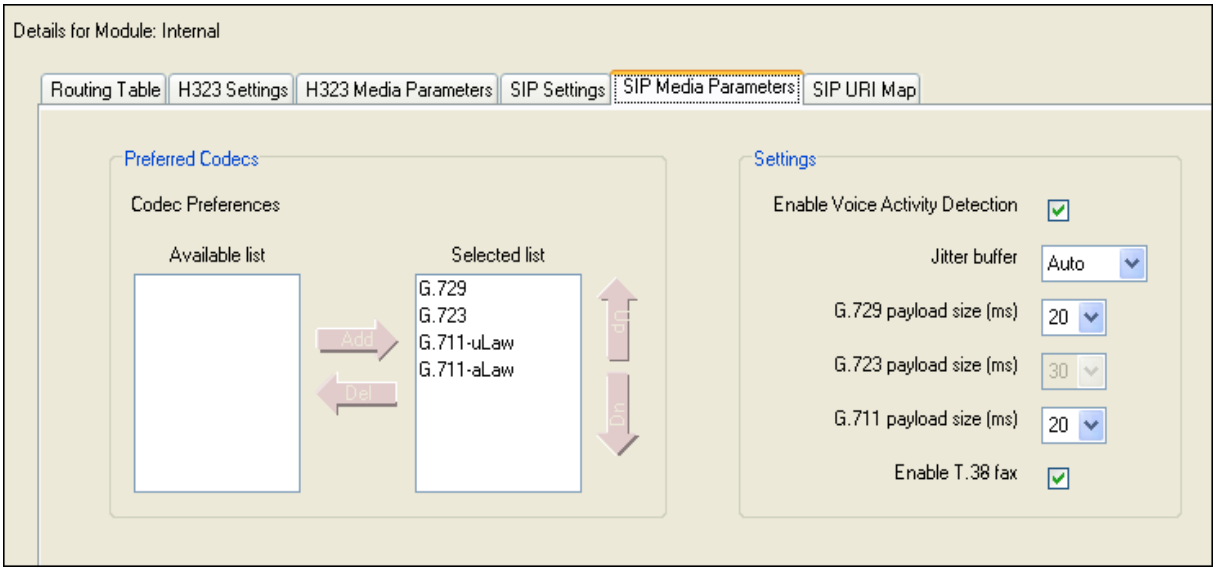


Table 25 SIP Media parameters tab (Sheet 1 of 2)

Field	Value	Description
Preferred Codecs		
Preferred Codecs	None G.711-uLaw G.711-aLaw G.729 G.723	Select the Codecs in the order in which you want the system to attempt to use them. **Performance note:** Codecs on all networked BCMs should be consistent to ensure that interacting features such as Transfer and Conference work correctly. **Note**: The G.723 codec can be used between IP endpoints. If other types of connections are required, ensure one of the other codecs is also selected.
Actions		
	1. On the Available list, click the codec you want to add to the Selected list. 2. Click the button to move the codec to the Selected list.	
	1. Select a codec that you want to remove from the Selected list. 2. Click this button to move the codec back to the Available list.	
	1. Select a codec on the Selected list. 2. Click the appropriate arrow to move the codec up or down in the Selected list.	

Table 25 SIP Media parameters tab (Sheet 2 of 2)

Field	Value	Description
Settings		
Enable Voice Activity Detection	<check box>	The voice activity detection (silence suppression) identifies periods of silence in a conversation, and stops sending IP speech packets during those periods. In a typical telephone conversation, most of the conversation is half-duplex, meaning that one person is speaking while the other is listening. For more information refer to "Silence suppression" on page 529. If voice activity detection is enabled, no voice packets are sent from the listener end. This greatly reduces bandwidth requirements. G.723.1 and G.729 support silence suppression. G.711 does not support silence suppression. **Performance note:** voice activity detection on all networked BCMs and IPT systems (VAD setting on IPT systems) must be consistent to ensure that interacting features such as Transfer and Conference work correctly. Default: Disabled
Jitter Buffer	Auto None Small Medium Large	Select the size of jitter buffer you want to allow for your system.
G.729 Payload Size (ms)	10, 20, 30, 40, 50, 60 Default: 30	Set the desired payload size, per codec, for VoIP calls sent over SIP trunks. **Note:** Payload size can also be set for Nortel IP telephones. Refer to the *Device Configuration Guide* (NN40020-300).Refer to the *Telephony Device Installation Guide* (NN40020-309).
G.723 Payload Size (ms)	30	
G.711 Payload Size (ms)	10, 20, 30, 40, 50, 60 Default: 30	
Enable T.38	<check box>	Enabled: The system supports T.38 fax over IP. Disabled: The system does not support T.38 fax over IP
		Caution: Operations note: Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference: Locate fax machine away from other telephones. Turn the speaker volume on the fax machine to the lowest level, or off, if that option is available.

SIP URI Map

Use the SIP URI Map to configure the sub-domain name associated with each SIP URI (Session Initiated Protocol Uniform Resource Identifier). These strings must be coordinated with the other nodes in the network.

Figure 34 SIP URI Map tab

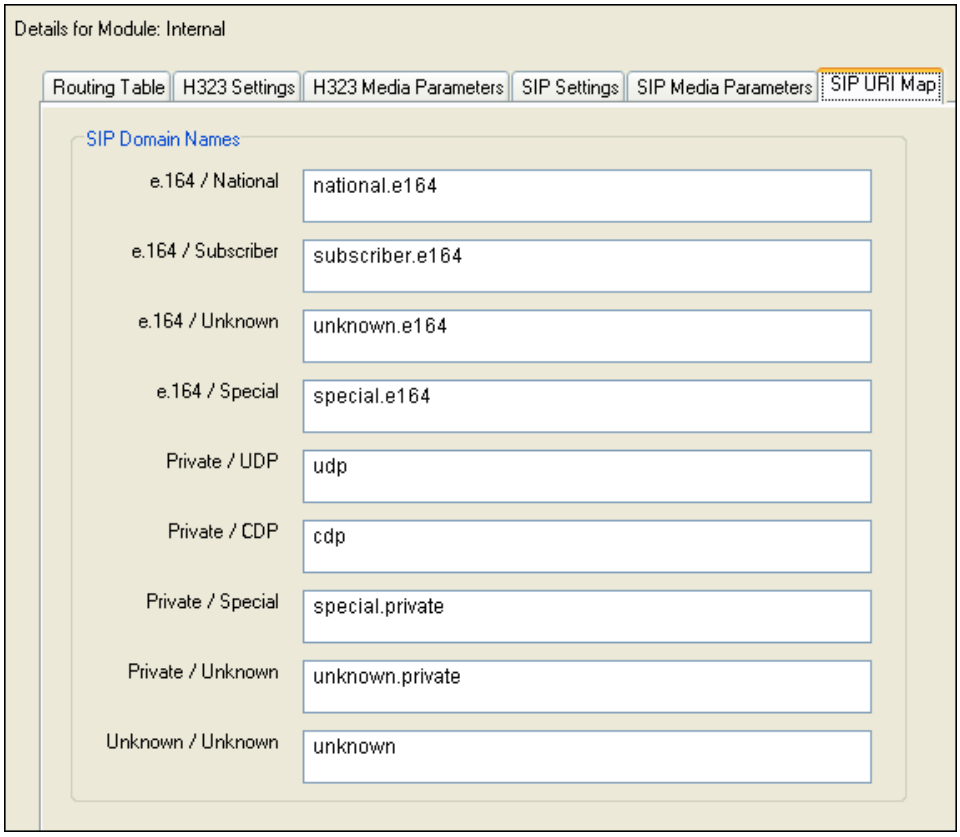


Table 26 SIP URI Map Fields

Field	Value	Description
SIP Domain Names		
e.164 / National	national.e164	String to use in phone context to identify numbering plan type
e.164 / Subscriber	subscriber.e164	String to use in phone context to identify numbering plan type
e.164 / Special	special.e164	String to use in phone context to identify numbering plan type
e.164 / Unknown	unknown.e164	String to use in phone context to identify numbering plan type
Private / UDP	UDP	String to use in phone context to identify numbering plan type
Private / CDP	CDP	String to use in phone context to identify numbering plan type
Private / Special	special.private	String to use in phone context to identify numbering plan type
Private / Unknown	unknown.private	String to use in phone context to identify numbering plan type
Unknown / Unknown	unknown	String to use in phone context to identify numbering plan type

Chapter 10
Configuring lines

All the Lines panels show the same type of tabbed panels. The information on the tabbed panels may vary, however, depending on the type of line.

The following paths indicate where to access the lines information in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

The top panel provides a table of lines and the current or default settings.

The bottom frame contains three tabs. The contents of the tabs may vary, depending on the line selected in the top table.

- The Properties tabbed panel provides the settings for individual line characteristics.
- The Restrictions tabbed panel allows you to define which restrictions will be active for individual lines. Note that lines that are assigned to the same line pool will automatically assign the same restrictions.
- The Assigned DNs tabbed panel provides a quick way to assign lines to telephones. You must use the DN records panels to assign line pools to telephones.

Click one of the following links to connect with the type of information you want to view:

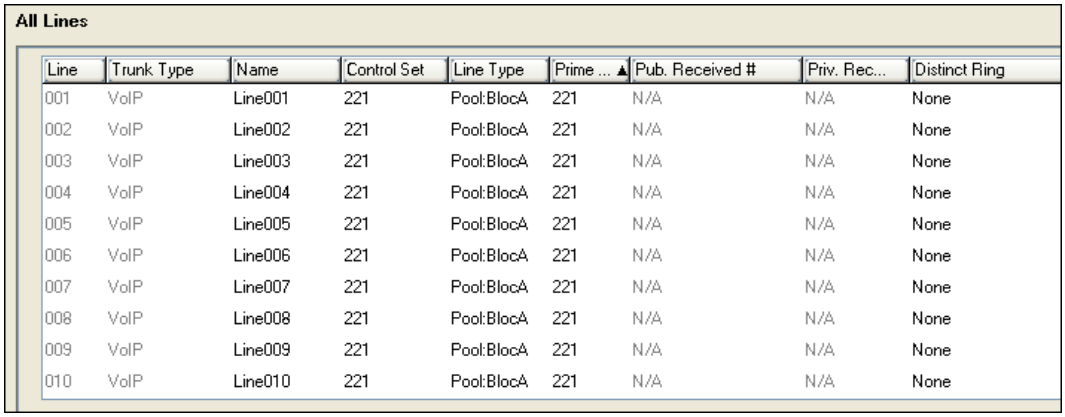
Panel tabs	Tasks
"Trunk/Line data, main panel" on page 130	"Configuring lines: T1-Loop start" on page 157
"Properties" on page 132	"Configuring lines: T1-Digital Ground Start" on page 163
"Restrictions (Line and Remote)" on page 137	"Configuring lines: T1-E&M" on page 151
"Assigned DNs" on page 138 See also: Line Access - Line Assignment tab in the *Device Configuration Guide* (NN40020-300)	"Configuring lines: T1-DID" on page 169
	"Configuring lines: PRI" on page 145
	"Configuring lines: DPNSS lines" on page 181
	"Configuring lines: Target lines" on page 141
	"Configuring BRI lines" on page 197
	"Configuring VoIP lines" on page 385
	"Call Security: Configuring Direct Inward System Access (DISA)" on page 427

Click the navigation tree heading to access general information about user management.

Trunk/Line data, main panel

The top-level Table View panel shows line records for all lines active on the system, and the common assigned parameters. Figure 35 shows the Trunk/Line Data lines panel.

Figure 35 Trunk/Line Data lines panel



Line	Trunk Type	Name	Control Set	Line Type	Prime ... ▲	Pub. Received #	Priv. Rec...	Distinct Ring
001	VoIP	Line001	221	Pool:BlocA	221	N/A	N/A	None
002	VoIP	Line002	221	Pool:BlocA	221	N/A	N/A	None
003	VoIP	Line003	221	Pool:BlocA	221	N/A	N/A	None
004	VoIP	Line004	221	Pool:BlocA	221	N/A	N/A	None
005	VoIP	Line005	221	Pool:BlocA	221	N/A	N/A	None
006	VoIP	Line006	221	Pool:BlocA	221	N/A	N/A	None
007	VoIP	Line007	221	Pool:BlocA	221	N/A	N/A	None
008	VoIP	Line008	221	Pool:BlocA	221	N/A	N/A	None
009	VoIP	Line009	221	Pool:BlocA	221	N/A	N/A	None
010	VoIP	Line010	221	Pool:BlocA	221	N/A	N/A	None

Table 27 describes the fields found on the Trunk/Line Data main panel.

Table 27 Trunk/Line Data main panel (Sheet 1 of 2)

Attribute	Value	Description
Line	This list contains all the possible line numbers for the system, including target lines.	Configure only those lines that are active on the system. (Click the Active check box and ensure that the Inactive check box is empty).
Trunk Type	Loop, PRI, VoIP, Target	There are three main categories of lines: PSTN-based lines: (analog, T1, PRI, BRI) Voice over IP (VoIP) trunks, which connect through the LAN or WAN. Target lines, which are internal channels that provide direct dial capability.
Name	<maximum of seven alphanumeric characters>	Identify the line in a way that is meaningful to your system, such as by the type of line and line pool or the DN it is attached to in the case of target line*s*.
Control Set	DN <control telephone DN> Default: 221 (default Start DN)	Enter a telephone DN for a telephone that you want to use to turn service off or on for other telephones using this line. The control telephone must have the line assigned, or must be assigned to the line pool the line is in. Refer to “Line Access - Line Pool Access tab” in the *Device Configuration Guide* (NN40020-300).
	Tips: External lines and telephones must be programmed to use one of the Scheduled Services: Ringing, Restriction, and Routing Services. For maximum flexibility, Nortel recommends that you create two different control telephones, one for the lines and one for the telephones. You can turn on a service manually or automatically for all external lines from an assigned control telephone. However, you cannot combine schedules. A service can only be active as normal service or one of the six schedules at any one time. Several schedules can be active at one time, but they must use different services.	
Line Type	Public Private to: Pool A to O, BlocA to BlocF	Define how the line is used in relation to other lines in the system. • Public line: can be accessed by more than one telephone. • Private line: can be assigned only to one telephone and the prime telephone for that line. Enter the internal number of the telephone. • Pool A - O (digital lines and BRI/BlocA to BlocF (PRI and VoIP lines): assigns the line to one of the line pools. If a line is assigned to a line pool, but is not assigned to any telephone, that line is available only for outgoing calls. Bloc line pools must be used in conjunction with routes and destination codes. Target line*s* cannot be put into line pools.

Table 27 Trunk/Line Data main panel (Sheet 2 of 2)

Attribute	Value	Description
Prime set	DN: None	Assign a telephone to provide backup answering for calls on the line. For an Auto Answer line, calls are redirected if the received number is invalid or the target line is busy, and if the **If busy** parameter is set **To prime**. Each line can be assigned only one prime telephone.
Pub. Received # (Target lines only)	<digits associated with a specific target line>	Specify the digits the system will use to identify a call from the public network to this target line. • A received number cannot be the same as, or be the start digits, of a line pool access code, a destination code, the DISA DN or the Auto DN. • If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. The call will be directed to the prime telephone for the incoming line if the Network DN is not used.
Priv. Received # (Target lines only)	<digits associated with a specific target line>	Specify the digits the system will use to identify a call from the private network to this target line. • A received number cannot be the same as, or be the start digits, of a line pool access code, a destination code, the DISA DN or the Auto DN. • If you are configuring auto-answer BRI trunks to map to target lines, the received number should be the same as the Network DN supplied by your service provider. The call will be directed to the prime telephone for the incoming line if the Network DN is not used.
Distinct ring	None Pattern 2 Pattern 3 Pattern 4	Choose the distinctive ring pattern that you want to assign to the line. This allows you to provide selective service to calls with differing answer priorities. When more than one line with the distinct ring settings rings at a telephone, the line with the highest priority rings first. • Pattern 4 has the highest ring priority • Pattern 3 has second highest ring priority • Pattern 2 has third highest ring priority • None has the lowest ring priority. By default, all telephones and lines are set to None.

Properties

The Properties tab shows basic line properties. Not all fields apply to all types of lines.

The Properties tab is shown in Figure 36 on page 133.

Figure 36 Properties details panel

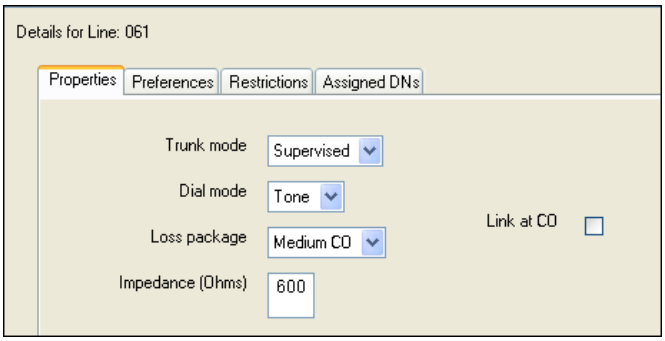


Table 28 defines the fields on this panel and indicates the lines.

Table 28 Properties line settings (Sheet 1 of 2)

Attribute	Value	Description
Legend: Loop = analog/digital loop; GS = ground start; DID = DID; E&M = E&M; BRI = BRI; DPNSS = DPNSS; VoIP = VoIP; TL = Target. Note: PRI fields are all included under the main table.		
Trunk mode	**Loop**	
	Unspr Supervised *Earth calling *Loop guarded *Loop unguarded	Define whether disconnect supervision, also referred to as loop supervision, releases an external line when an open switch interval (OSI) is detected during a call on that line. You must set this to Supervised if a loop trunk has its Answer mode set to Auto or if you enable Answer with DISA. Disconnect supervision is also required to conference two external callers. The line must be equipped with disconnect supervision from the central office for the Supervised option to work. * These listing only appear for UK analog lines.
Dial mode	**Loop** **GS**	**DID** **E&M**
	Pulse Tone	Specify whether the system uses dual tone multifrequency (DTMF) or pulse signaling on the trunk. Tone does not appear if Signaling is set to Immediate (T1 DID &T1 E&M trunk types only).
Loss package	**Loop (analog only)**	
	Short CO Medium CO Long CO Short PBX Long PBX	Select the appropriate loss/gain and impedance settings for each line, see Table 12.
Impedance (Ohms)	**Loop (analog only)**	
	600 ohm-900 ohm	The GATM can be set to a specific impedance level.

Table 28 Properties line settings (Sheet 2 of 2)

Attribute	Value	Description
Legend: Loop = analog/digital loop; GS = ground start; DID = DID; E&M = E&M; BRI = BRI; DPNSS = DPNSS; VoIP = VoIP; TL = Target. Note: PRI fields are all included under the main table.		
Line Tuning Digit	**Loop (analog only)**	
	<drop-down menu>, none 0-9	If the **Line Tuning Digit** dropdown list is cleared, line tuning is disabled. Otherwise, line tuning is enabled. By default the digit used to remove dial tone is 1. In most configurations, the digit 1 is sufficient to remove dial tone so that line tuning can execute. In the rare case where the central office requires an alternate digit, the technician can choose a digit other than 1.
Signaling	**DID**	**E&M**
	WinkStart Immediate DelayDial	Select the signal type for the line. The immediate setting does not appear for T1 E&M or T1 DID trunks connected to a DTM if the Dial mode is set to tone. Make sure that this matches the signal type programmed for the trunk at the other switch.
Link at CO	**Loop (analog only)**	
	<check box>	Some exchanges respond to a Link signal, also called hook flash (**FEATURE 71**), by providing an alternative line for making outgoing calls. Enabling Link at CO causes the system to apply the restrictions on outgoing calls to the digits dialed after the Link signal. As well, the call on the alternative line is subject to all restrictions. Disabling Link at CO prevents a Link signal from resetting the BCM restrictions in cases where the host exchange does not provide an alternative line.

Preferences (lines)

The Preferences tab shows information that may vary from trunk to trunk. Most of this information needs to coordinate with the line service provider equipment.

The Preferences tab is shown in Figure 37.

Figure 37 Preferences details panel

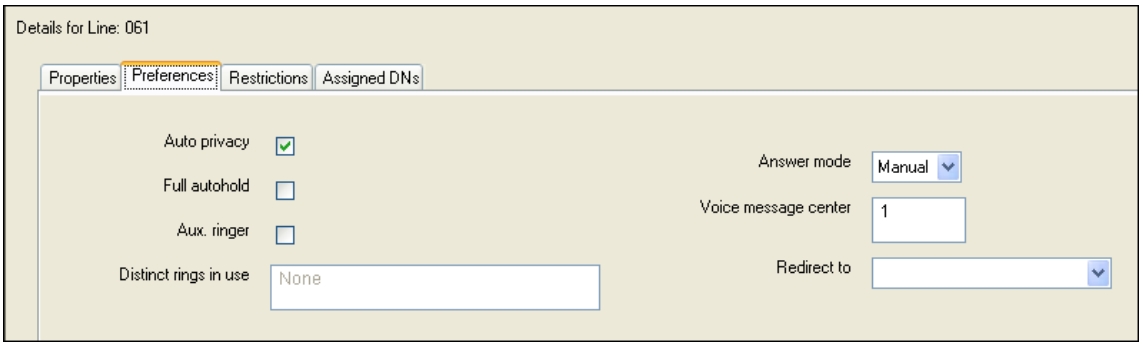


Table 29 defines the fields on this panel and indicates the lines.

Table 29 Preferences details fields for lines (Sheet 1 of 3)

Attribute	Value	Description
Legend: Loop = analog/digital loop; GS = ground start; DID = DID; E&M = E&M; BRI = BRI; DPNSS = DPNSS; VoIP = VoIP; TL = Target and DASS2. Note: PRI fields are all included under the main panel.		
Auto privacy	**Loop** **GS** **DID** **E&M** **BRI** **VoIP**	
	<check box>	Define whether one BCM user can select a line in use at another telephone to join an existing call. Refer to “Turn Privacy on or off” in the *Device Configuration Guide* (NN40020-300) (**FEATURE** 83).
Full autohold	**Loop** **BRI** **DPNSS** **VoIP**	
	<check box>	Enables or disables Full autohold. When enabled, if a caller selects an idle line but does not dial any digits, that line is automatically placed on hold if you then select another line. Full autohold is always in place for T1 E&M trunks because it has no meaning for incoming-only T1 DID trunks. The default setting should be changed only if Full autohold is required for a specific application.
Aux. ringer	**Loop** **GS** **DID** **E&M** **BRI** **DPNSS** **VoIP** **TL**	
	<check box>	Turn the auxiliary ringer on or off for all telephones using this line. When programmed on a line, the auxiliary ringer will ring every time a call is received.
	Note: When programmed only on a telephone, no ring occurs for a transferred call. An auxiliary ringer can also be programmed in Services to ring for a line placed into a scheduled Ringing service. Refer to “Configuring scheduled service” in the *Device Configuration Guide* (NN40020-300).	

Table 29 Preferences details fields for lines (Sheet 2 of 3)

Attribute	Value	Description
Legend: Loop = analog/digital loop; GS = ground start; DID = DID; E&M = E&M; BRI = BRI; DPNSS = DPNSS; VoIP = VoIP; TL = Target and DASS2. Note: PRI fields are all included under the main panel.		
ANI Number	**DID** **E&M**	
	<check box>	Define whether the telephone number of the caller will be shown for this line. For T1 E&M and T1 DID trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart. The central office must deliver ANI/DNIS in DTMF mode. No additional equipment is required.
DNIS Number	**E&M**	
	<check box>	Defines whether the digits dialed by an external caller on this line will be shown.For T1 E&M trunks connected to a DTM, this setting only appears if Signaling is set to WinkStart and Answer mode is set to Manual.
Distinct Rings in use	<read-only>	Indicates if a special ring has been assigned. See Distinct Ring on the main table.
Answer mode	**Loop** **GS** **E&M** **BRI** **DPNSS**	
	Manual Auto	Define whether a trunk is manual or automatic answer. Auto answer mode allows the trunk to be a shared resource by the system telephones. This shared resource is created through routing to target lines or using DISA. For auto answer trunks being used to allow remote call-in from system users, the trunk can be configured to answer with a straight dial tone, if DISA has not been enabled. It can also be configured to answer with a stuttered dial tone if DISA is enabled and the caller is expected to enter a CoS password. The CoS password defines which system features the caller is permitted to access. Manual answer trunks are assigned to one or more telephones. The assigned telephones exclusively own the line.
	Note: You require Disconnect supervision on the line if loop start trunks are to operate in auto-answer mode.	
Answer with DISA	**Loop** **GS** **E&M** **BRI**	
	<check box>	Define whether the system prompts a caller for a six-digit class of service (CoS) password. This setting appears for T1 loop start, T1 E&M lines that have auto-answer mode, and analog trunks. Set this option to No for T1 E&M lines on a private network that have auto-answer mode. To program DISA on a PRI trunk you need to specify a DISA DN, see “Call Security: Configuring Direct Inward System Access (DISA)” on page 427 and “Dialing plan: Private network settings” on page 281.

Table 29 Preferences details fields for lines (Sheet 3 of 3)

Attribute	Value		Description					
Legend: Loop = analog/digital loop; GS = ground start; DID = DID; E&M = E&M; BRI = BRI; DPNSS = DPNSS; VoIP = VoIP; TL = Target and DASS2. Note: PRI fields are all included under the main panel.								
If busy								**TL**
	To Prime Busy Tone		Define whether a caller receives a busy tone or the call forwards to the prime telephone when the target line is busy. Busy tone only works for PRI trunks.					
	Tips: The duration of an open switch interval (OSI) before BCM disconnects a call is programmed by the Disconnect timer setting. Refer to "Trunk Module Parameters" on page 104.							
Voice Message Center	**Loop**	**GS**	**DID**	**E&M**	**BRI**	**DPNSS**	**VoIP**	**TL**
	Center 1 - Center 5		If this line connects t o a remote voice mail, either through the private network or at the Central Office, indicate which Center number has been configured with the contact number.The system calls that number to check voice mail messages when a message indicator is presented to a telephone.					
Redirect to	**Loop**	**GS**	**DID**	**E&M**				**TL**
	<dial string>		Enter a dial string (including destination code) to redirect the line to an external telephone, such as a call attendant on another system. If you want to stop redirection, you need to delete the dial string and allow the record to update. **Warning**: If the dialstring is set up, the line will immediately be redirected out of the system not ringing any telephone.					
Warning: Enable modules If you disabled any trunk media bay modules prior to performing programming, enable them now to ensure your system will function properly.								

Restrictions (Line and Remote)

Assigning Line restrictions and Remote Access Package restrictions are part of the configuration for controlling calls out of the system (line restrictions) and into the system from a private network node or from a remote user calling in over the PSTN lines (Remote Access Packages).

The following paths indicate where to access the restriction settings in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface:****CONFIG > Lines** or ****CONFIG > Terminals and Sets**

The Restrictions tab is shown in Figure 38.

Figure 38 Restrictions tables for a line

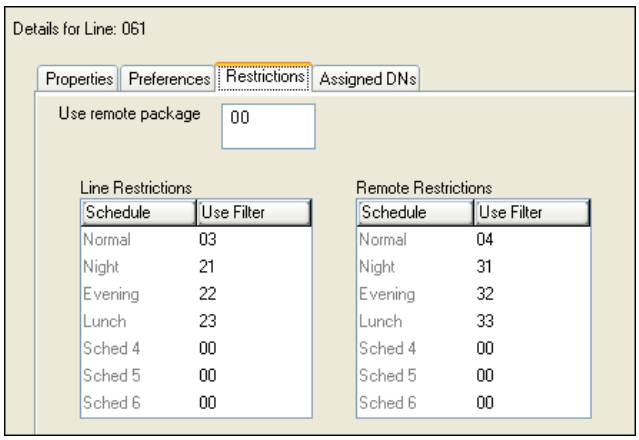


Table 30 describes the fields on this panel.

Table 30 Restrictions

Attribute	Values	Description
Use remote package	<remote package #>	If the line is being used to receive external calls or calls from other nodes on the private network, ensure that you indicate a remote package that provides only the availability that you want external callers to have. This attribute is typically used for tandeming calls.
Schedule	Default: Normal, Night, Evening, Lunch, Sched 4, Sched 5, Sched 6	
Line Restrictions - Use Filter	<00-99>	Enter the restriction filter number that applies to each schedule. (controls outgoing calls)
Remote Restrictions - Use Filter	<00-99>	Enter the restriction filter that applies to each schedule. This setting provides call controls for incoming calls over a private network or from remote user dialing in over PSTN)

Assigned DNs

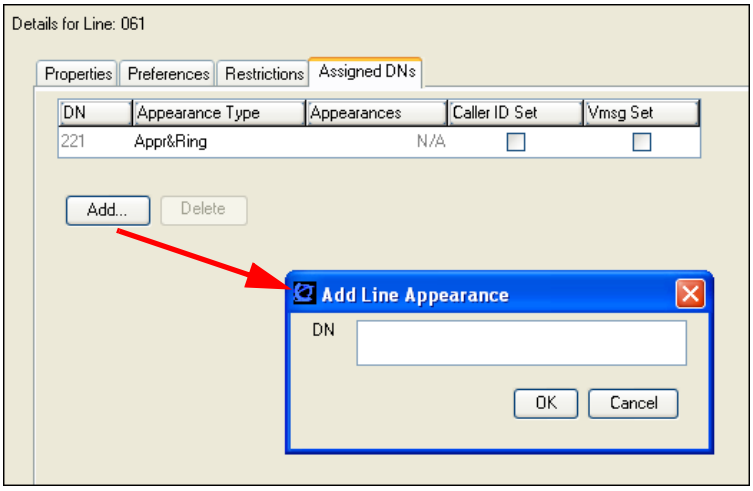
The Assigned DNs tabbed panel displays the DN properties for lines that are assigned to telephones.

This information can also be configured on the DN record. Any information added, deleted or modified in this table reflects in the DN record.

Note: Lines that do not allow single-line assignment, such as PRI lines and VoIP lines, will not display this tabbed panel.

The Assigned DNs tab is shown in Figure 39.

Figure 39 Add a DN record



To add a DN record to a line record

1 In the top panel, click the line where you want to add a DN record.

2 In the bottom frame, click **Add**.

3 Enter the DN record number and line settings:

- DN
- Appearance Type
- Appearances (target lines only)
- Caller ID Set (for display sets and ASM8+)
- VMsg Set

4 Click **OK**.

5 Repeat for all the DN records you want to assign.

Chapter 11
Configuring lines: Target lines

Target lines are virtual lines that allow the mapping of received digits to a line number over PRI channel.

The following paths indicate where to access target lines in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: Configure Target lines and DASS2 line settings

• "Configuring Target line settings" on page 144

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

Ensure that external number is mapped to internal received number, if required.	
Have a list of DNs where the target lines will get assigned.	
For features that require target lines: • Configure lines into line pools. Refer to "Trunk Module Parameters" on page 104. • Routing and destination codes. Refer to "Dialing plan: Routing and destination codes" on page 259. • Set up VoIP fallback. Refer to "Setting up VoIP trunks for fallback" on page 391.	

Process map

Figure 40 and Figure 41 provide an overview of the target line feature configuration process.

Figure 40 Configuring target lines — main screen

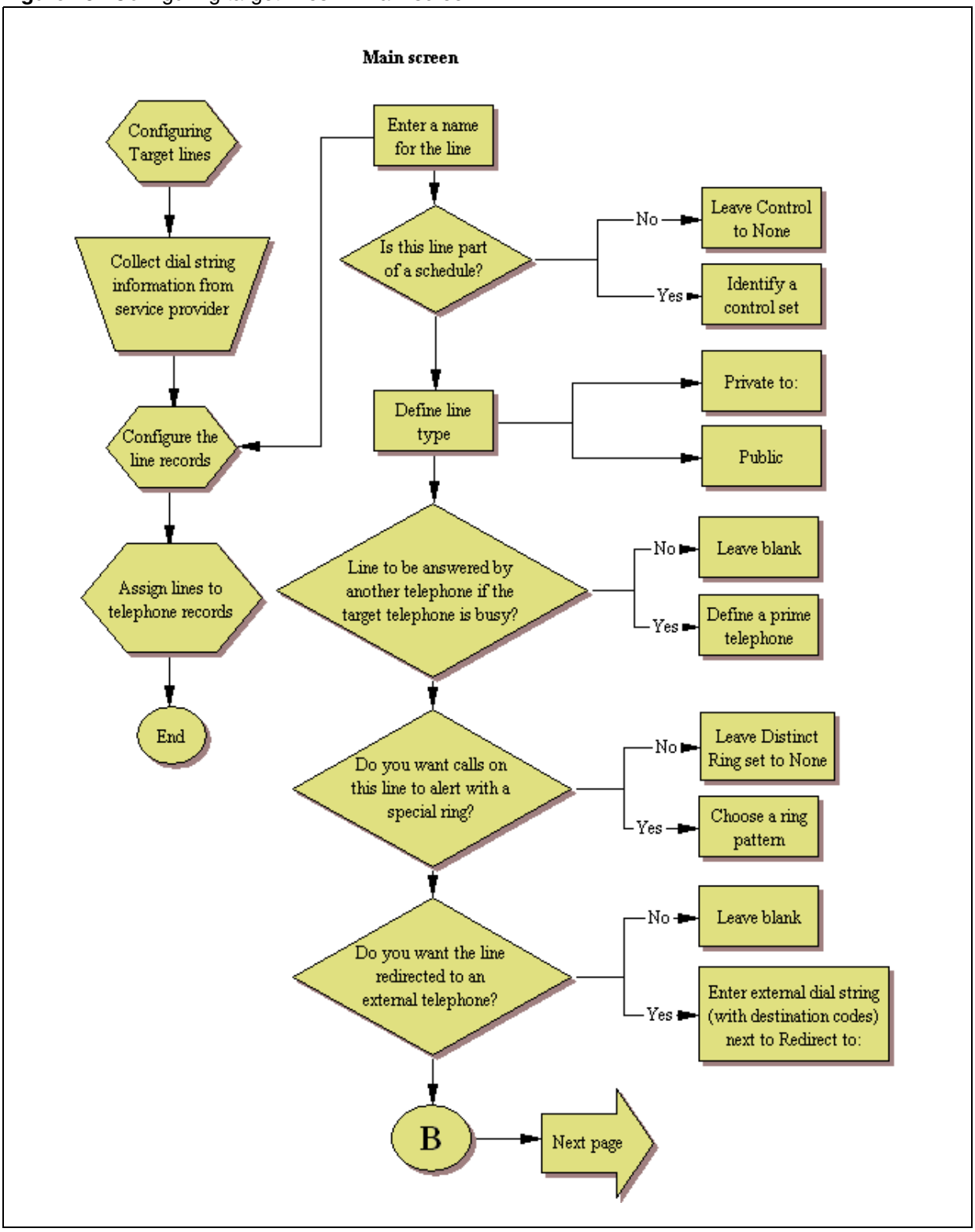
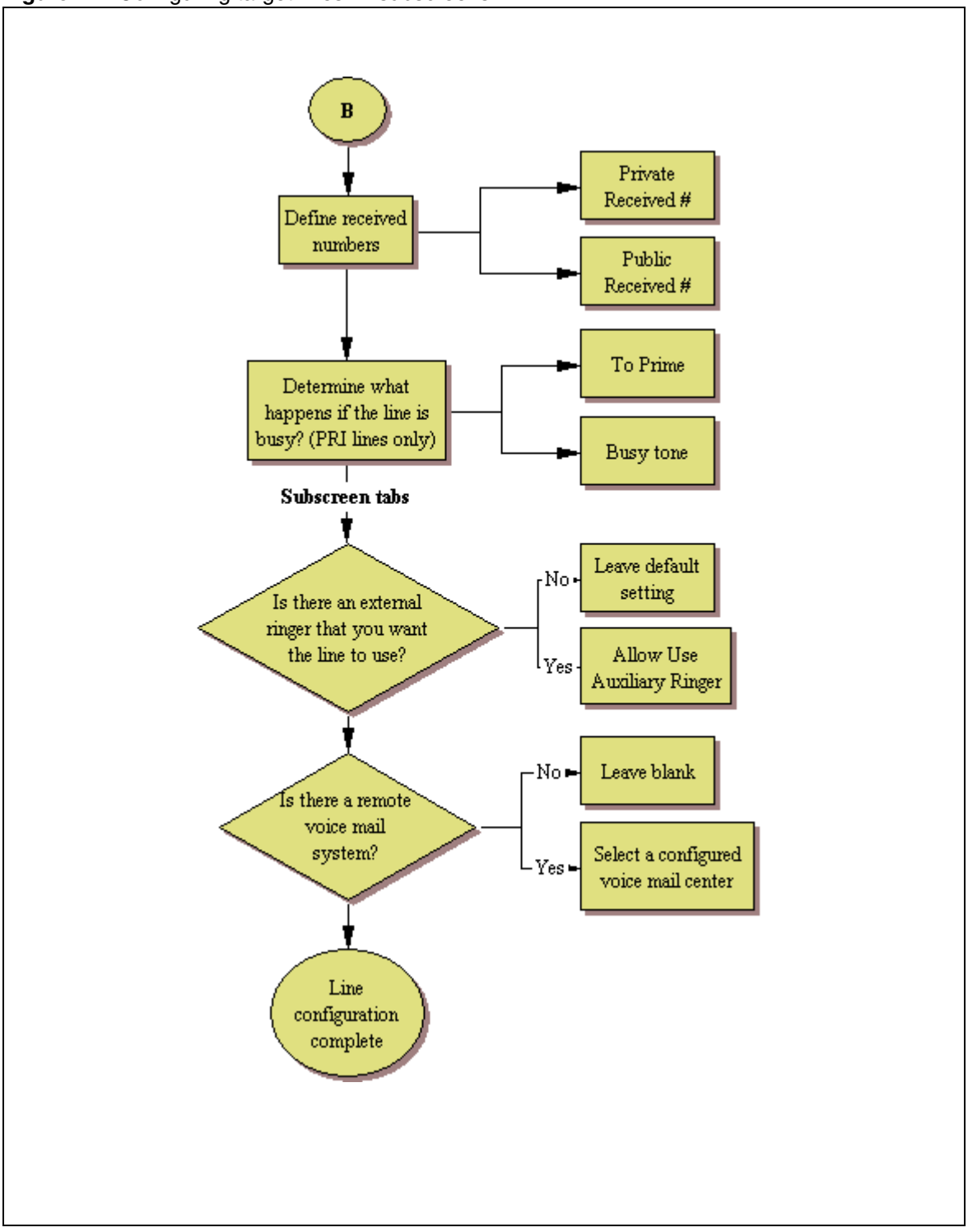


Figure 41 Configuring target lines — subscreens



Configuring Target line settings

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Line: Number of the assigned line.
- Trunk Type: Target line.
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.
- Line Type: Set to Public, if the line is to be shared among telephones or DN:*: if the line is only assigned to one telephone.
- Prime Set: If the line is to be answered at another telephone if the line is not answered at the target telephone.
- Pub. Received #: Confirm the existing number or enter a public received # (PSTN DID or PRI trunks) that the system will recognize as the target telephone/group.
- Private Received #: If private network trunks (PRI or VoIP trunks) are configured, enter a Private received #. This number is usually the same as the DN.
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).

2 Configure the trunk/line data (Preferences tab):

- Aux. ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- If Busy: To automatically direct calls to the prime telephone, select To prime from the drop-down menu, or select Busy tone.
- Voice message center: If the system is using a remote voice mail, select the center configured with the contact number.
- Redirect to: To automatically direct calls out of the system to a specific telephone, such as a headoffice answer attendant, enter that remote number here. Ensure that you include the proper routing information.

3 Assign the lines to DNs (see "Assigned DNs" on page 138):

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs here. The DN record can also be used to assign lines; refer to "Line Access - Line Assignment tab in the *Device Configuration Guide* (NN40020-300).

- DN: Unique number.
- Appearance Type: Choose Appr only or Appr&Ring if the telephone has an available button, otherwise choose Ring only.
- Appearances: Target lines can have more than one appearance, so that multiple calls can be accommodated. For telephones that have these lines set to Ring only, set to None.
- Caller ID Set: Select check box to display caller ID for calls coming in over the target line.
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting. Check with your system administrator for the system voice mail setup before changing this parameter.

Chapter 12
Configuring lines: PRI

PRI are auto-answer lines. These lines cannot be individually assigned to telephones. They must be configured into line pools. PRI line pools then are assigned routes and these routes are used to create destination codes.

The following paths indicate where to access PRI line pools in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: Configure the PRI lines connected to the system

- "Configuring PRI line features" on page 147
- "Configuring PRI Call-by-Call services" on page 148

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

Install and configure the DTM module. Refer to "Trunk Module Parameters" on page 104.	
Provision lines. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 42 and Figure 43 provide an overview of the PRI line feature configuration process.

Figure 42 PRI line feature configuration process — Part A

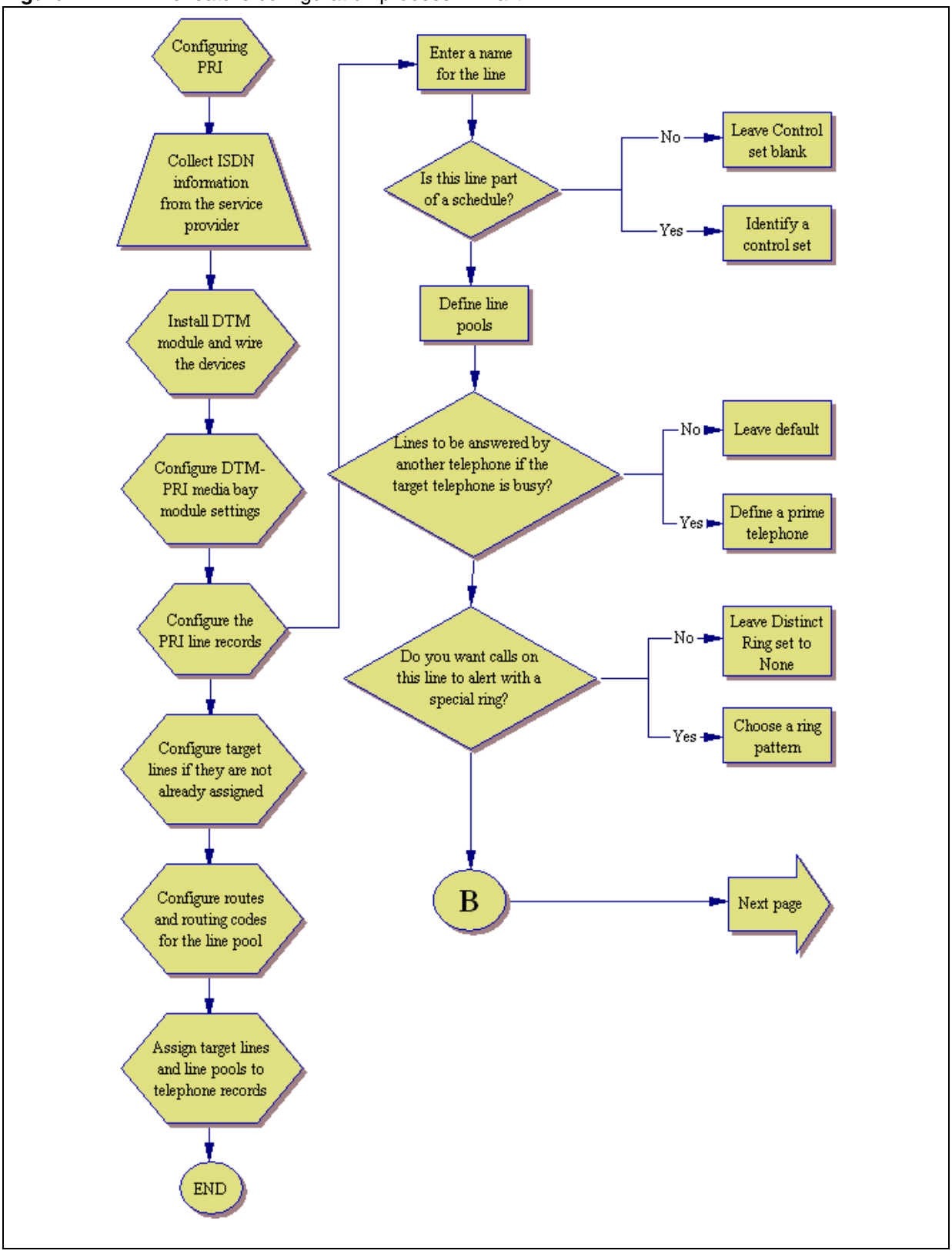
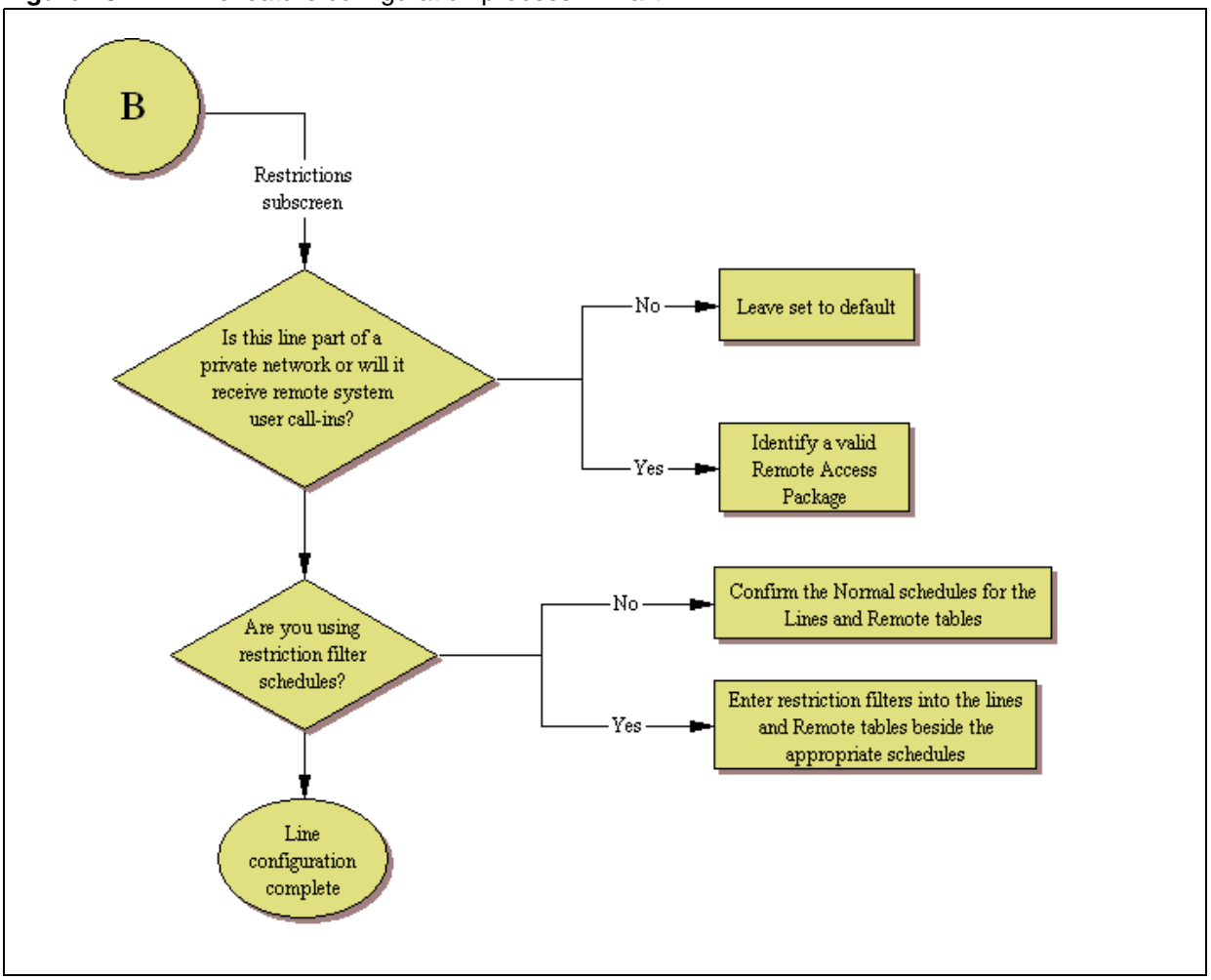

Configuring PRI
Collect ISDN information from the service provider
Install DTM module and wire the devices
Configure DTM-PRI media bay module settings
Configure the PRI line records
Configure target lines if they are not already assigned
Configure routes and routing codes for the line pool
Assign target lines and line pools to telephone records
END
Enter a name for the line
Is this line part of a schedule?
No
Leave Control set blank
Yes
Identify a control set
Define line pools
Lines to be answered by another telephone if the target telephone is busy?
No
Leave default
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Leave Distinct Ring set to None
Yes
Choose a ring pattern
B
Next page

Figure 43 PRI line feature configuration process — Part B


B
Restrictions subscreen
Is this line part of a private network or will it receive remote system user call-ins?
No
Leave set to default
Yes
Identify a valid Remote Access Package
Are you using restriction filter schedules?
No
Confirm the Normal schedules for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Line configuration complete

Configuring PRI line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Line: Number of the line being assigned.
- Trunk Type: PRI or ETSI (European standard).
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.
- Line Type: Define how the line will be used. If you are using routing, ensure it is put into line pool (BlocA to BlocF). If you use line pools, you need to assign target lines to the telephones, as well (refer to "Configuring lines: Target lines" on page 141).
- Prime Set: If you want the line to be answered at another telephone, if the line is not answered at the target telephone.

- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).

Subpanel under Restrictions tab:

- Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid package.

These lines cannot be assigned to DNs as line assignments. They are assigned only as line pools. Instead, configure target lines for each telephone and assign the target line to the telephones. For more information, refer to the *Device Configuration Guide* (NN40020-300).

2 Suggested next steps:

- Dialing plan
  "Dialing plan: System settings" on page 267
  "Dialing plan: Public network" on page 275
  "Dialing plan: Private network settings" on page 281
  "Dialing plan: Routing and destination codes" on page 259
- Networking
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339
  "Private networking: PRI Call-by-Call services" on page 343
  "Private networking: PRI and VoIP tandem networks" on page 323
  "Private networking: MCDN and ETSI network features" on page 319
  "Private networking: MCDN over PRI and VoIP" on page 297

Configuring PRI Call-by-Call services

Call-by-Call service selection (CbC) allows you to access services or private facilities over a PRI line without the need for dedicated facilities. The different services represent different types of access to the network.

The following protocols support Call-by-Call limits:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250
- AT&T 4ESS custom

There are several areas in the interface where you need to configure Call-by-Call services and the PRI lines that support these services.

To configure Call-by-Call services and the PRI lines

1. Set up the DTM module to support PRI.
2. Set up the Call-by-Call services selection for the module. Refer to "Call-by-Call Service Selection" on page 108.
3. Provision the PRI lines. Refer to "Provisioning module lines/loops" on page 112.
4. Configure the PRI lines. Refer to "Configuring lines: PRI" on page 145.
5. Configure target lines, if they are not already configured for your system. Refer to "Configuring lines: Target lines" on page 141.
6. Assign the PRI line pools to telephones. Refer to "Line Access - Line Pool Access tab in the *Device Configuration Guide* (NN40020-300)".
7. Assign the target lines to telephones. Refer to "Line Access - Line Pool Access tab in the *Device Configuration Guide* (NN40020-300)" and "Line pools: DNs tab in the *Device Configuration Guide* (NN40020-300)".
8. Set up routing for the PRI pools. Refer to "Programming the PRI routing table" on page 255.
9. Set up call-by-call limits for the line pools. Refer to "Line pools: Call-by-Call Limits tab (PRI only)" on page 360. Set up routing scheduling for the PRI line pools.

Chapter 13
Configuring lines: T1-E&M

E&M lines must be digital (T1).

The following paths indicate where to access the E&M lines in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: Configure T1 E&M lines connected to the system

• "Configuring E&M line features" on page 155

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

DTM module: Installed and configured. Refer to "Trunk Module Parameters" on page 104.	
Lines are provisioned. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 44, Figure 45, and Figure 46 provide an overview for configuring the line features for T1-E&M lines.

Figure 44 T1-E&M line configuration process — Part A

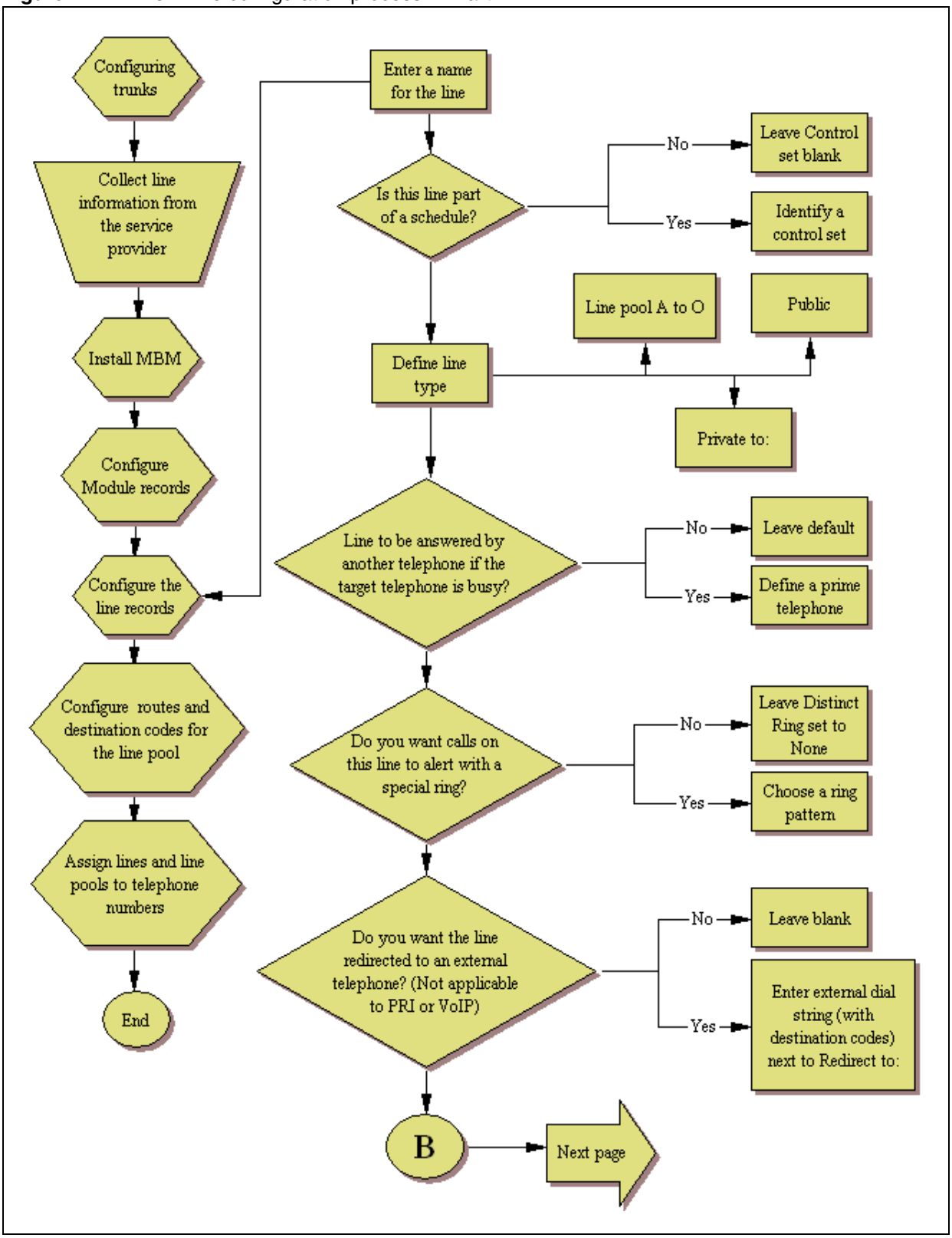

Configuring trunks
Collect line information from the service provider
Install MBM
Configure Module records
Configure the line records
Configure routes and destination codes for the line pool
Assign lines and line pools to telephone numbers
End
Enter a name for the line
Is this line part of a schedule?
No
Leave Control set blank
Yes
Identify a control set
Define line type
Line pool A to O
Public
Private to:
Line to be answered by another telephone if the target telephone is busy?
No
Leave default
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Leave Distinct Ring set to None
Yes
Choose a ring pattern
Do you want the line redirected to an external telephone? (Not applicable to PRI or VoIP)
No
Leave blank
Yes
Enter external dial string (with destination codes) next to Redirect to:
B
Next page

Figure 45 T1-E&M line configuration process — Part B

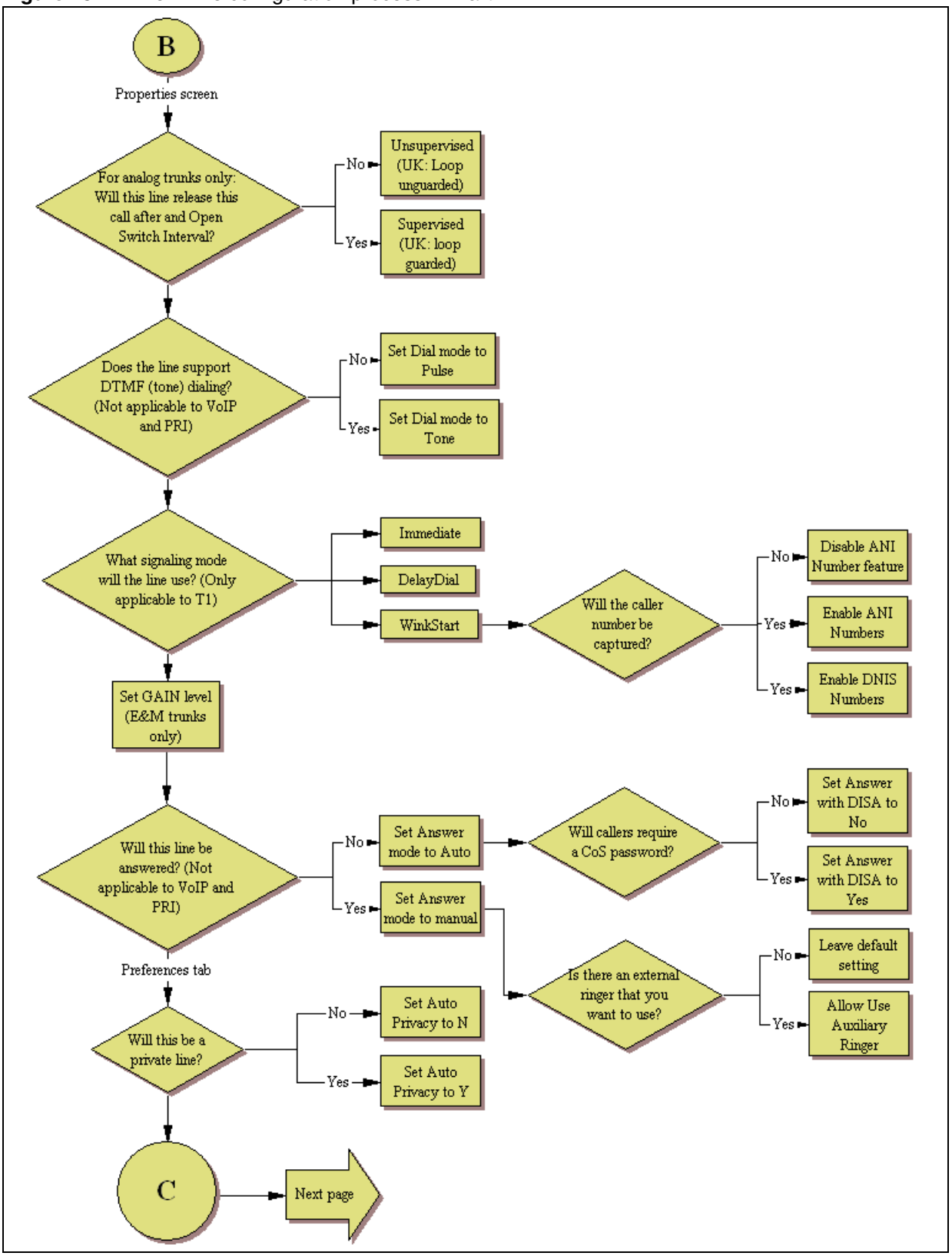
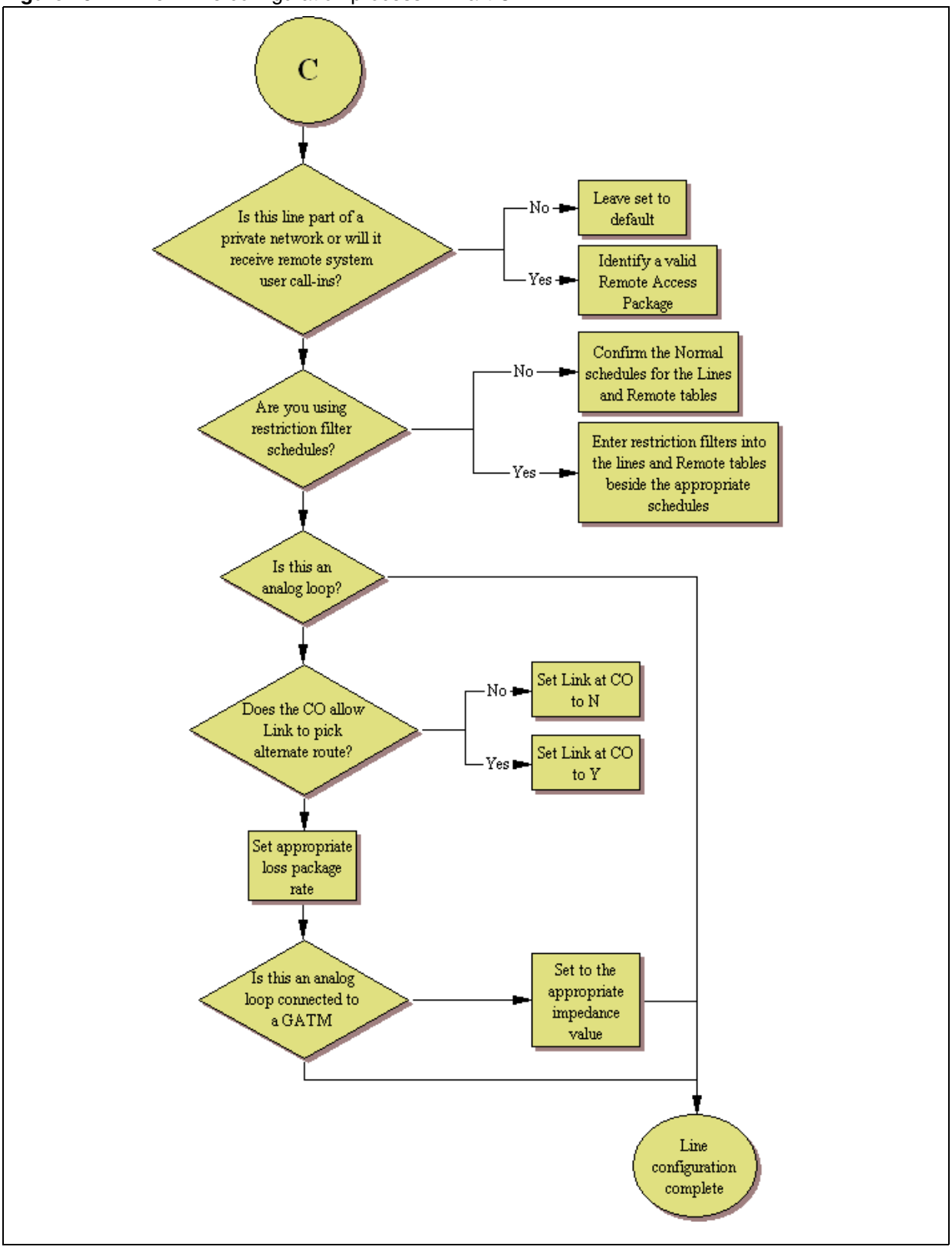


Figure 46 T1-E&M line configuration process — Part C


C
Is this line part of a private network or will it receive remote system user call-ins?
No
Leave set to default
Yes
Identify a valid Remote Access Package
Are you using restriction filter schedules?
No
Confirm the Normal schedules for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Is this an analog loop?
Does the CO allow Link to pick alternate route?
No
Set Link at CO to N
Yes
Set Link at CO to Y
Set appropriate loss package rate
Is this an analog loop connected to a GATM
Set to the appropriate impedance value
Line configuration complete

Configuring E&M line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Line: Line number.
- Trunk Type: E&M.
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.
- Line Type: Define how the line will be used. If you are using routing, ensure it is put into line pool (A to O). If you use line pools, you also need to configure target lines and assign the target lines to DNs. Refer to "Configuring Target line settings" on page 144.
- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, or 4).
- Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid package.

2 Configure the trunk/line data (Properties tab):

- Dial mode: The line service dictates whether this needs to be set to Pulse or Tone (DTMF) dialing. These are the only two options available.
- Signaling: Match this choice with the information supplied by the service provider.

3 Set the preferences (Preferences tab):

- Auto privacy: If you activate this feature, the line is available only to the telephone that answers the call.
- Aux. ringer: Use if your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- ANI number: Enable if the caller number is to be logged. For T1 lines, this only appears if Signaling is set to WinkStart.
- DNIS number: Defines whether the digits dialed by an external caller on this line will be shown.
- Answer mode: If this line is used for remote call-ins, determine how you want the line to answer (Auto or Manual). If the answer mode is set to Auto, decide whether the caller will be immediately connected to the system or whether a stuttered dial tone will require the caller to enter a CoS password.
- Voice message center: If the system is using a remote voice mail, select the center configured with the contact number.
- Distinct rings: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).

- Redirect to: If you want to automatically direct calls out of the system to a specific telephone, such as a headoffice answer attendant, enter that remote number here. Ensure that you include the proper routing information.

4 Set the restriction and remote package scheduling (Restrictions tab):

- Use remote package: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)
- Line restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Restrictions: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

5 Assign the lines to DNs (Assigned DNs tab) (applicable to manual answer only)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs, here. The DN record also can be used to assign lines and line pools for these lines.

- DN: Unique number.
- Appearance type: Choose Appr or Appr&ring if the telephone has an available button, otherwise choose Ring only. Model 7000 and 7100 telephones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- Vmsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting. Check with your system administrator for the system voice mail setup before changing this parameter.

6 Suggested next steps:

- Dialing plan
  "Dialing plan: System settings" on page 267
  "Dialing plan: Public network" on page 275
  "Dialing plan: Routing and destination codes" on page 259)
- Networking
  "Public networking: Setting up basic systems" on page 289
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339

Chapter 14
Configuring lines: T1-Loop start

Loop start trunks provide remote access to the BCM from the public network. They must be configured to auto-answer to provide remote system access. A loop start trunk must have disconnect supervision if it is to operate in the auto-answer mode.

The following paths indicate where to access the loop start trunks information through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: Configure the analog or digital loop start lines connected to the system.

• "Configuring digital (T1/E1) loop start lines" on page 161

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

Analog or DTM module is installed and configured. Refer to "Trunk Module Parameters" on page 104.	
Lines are provisioned. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 47, Figure 48, and Figure 49 provide an overview of the configuration process for T1-Loop start lines.

Figure 47 T1-Loop start line configuration process — Part A

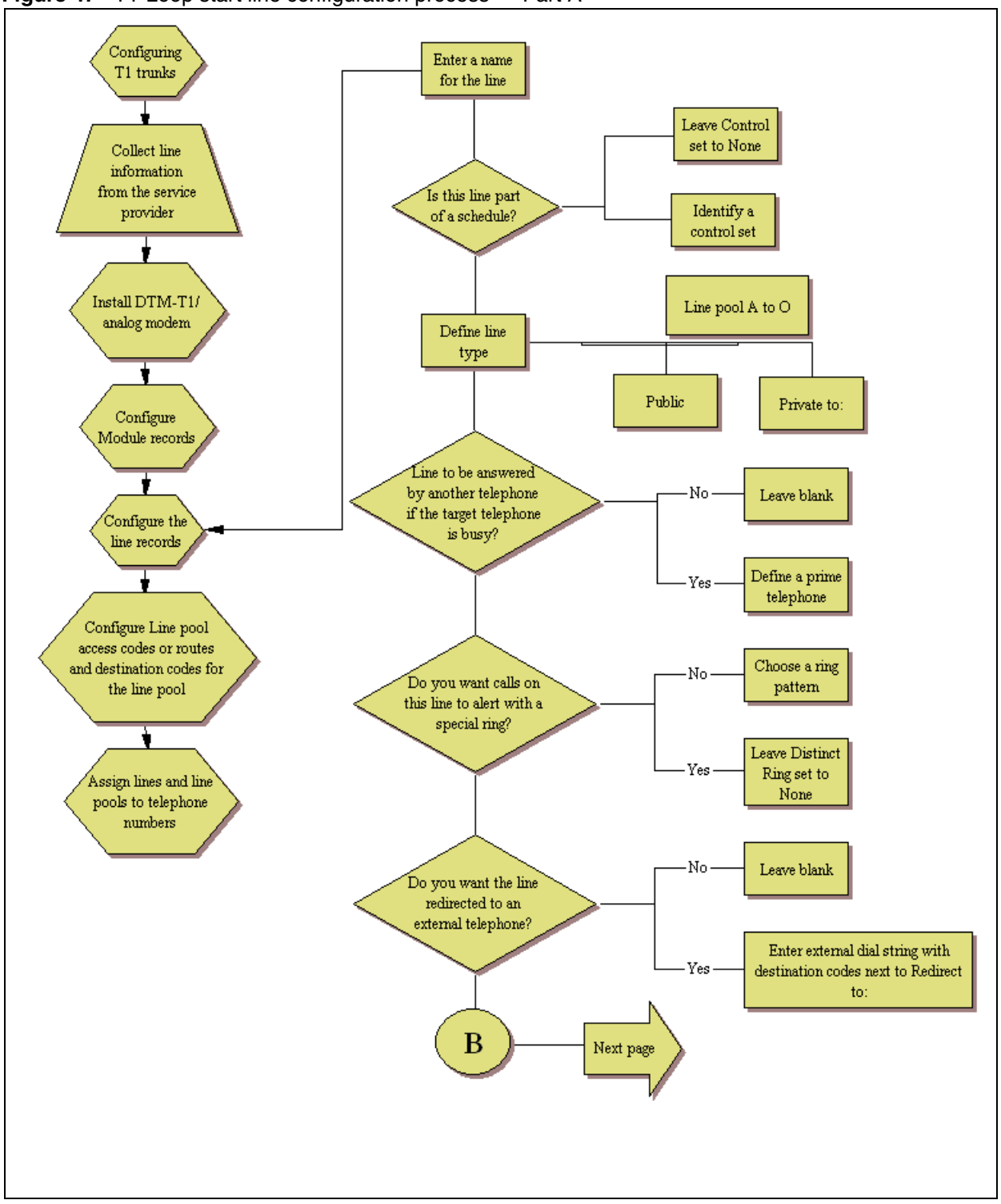

Configuring T1 trunks
Collect line information from the service provider
Install DTM-T1/ analog modem
Configure Module records
Configure the line records
Configure Line pool access codes or routes and destination codes for the line pool
Assign lines and line pools to telephone numbers
Enter a name for the line
Is this line part of a schedule?
Leave Control set to None
Identify a control set
Define line type
Line pool A to O
Public
Private to:
Line to be answered by another telephone if the target telephone is busy?
No
Leave blank
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Choose a ring pattern
Yes
Leave Distinct Ring set to None
Do you want the line redirected to an external telephone?
No
Leave blank
Yes
Enter external dial string with destination codes next to Redirect to:
B
Next page

Figure 48 T1-Loop start line configuration process — Part B

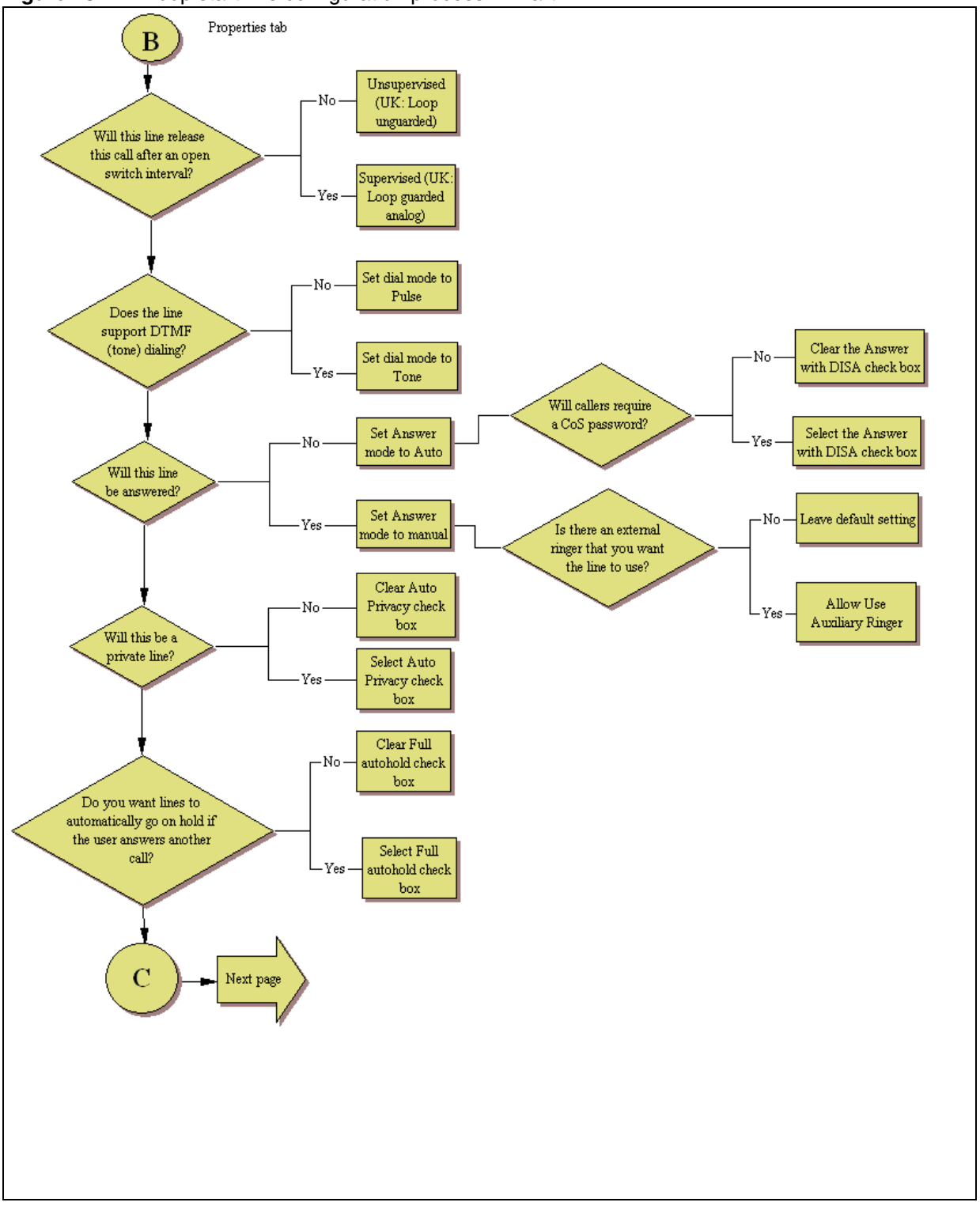
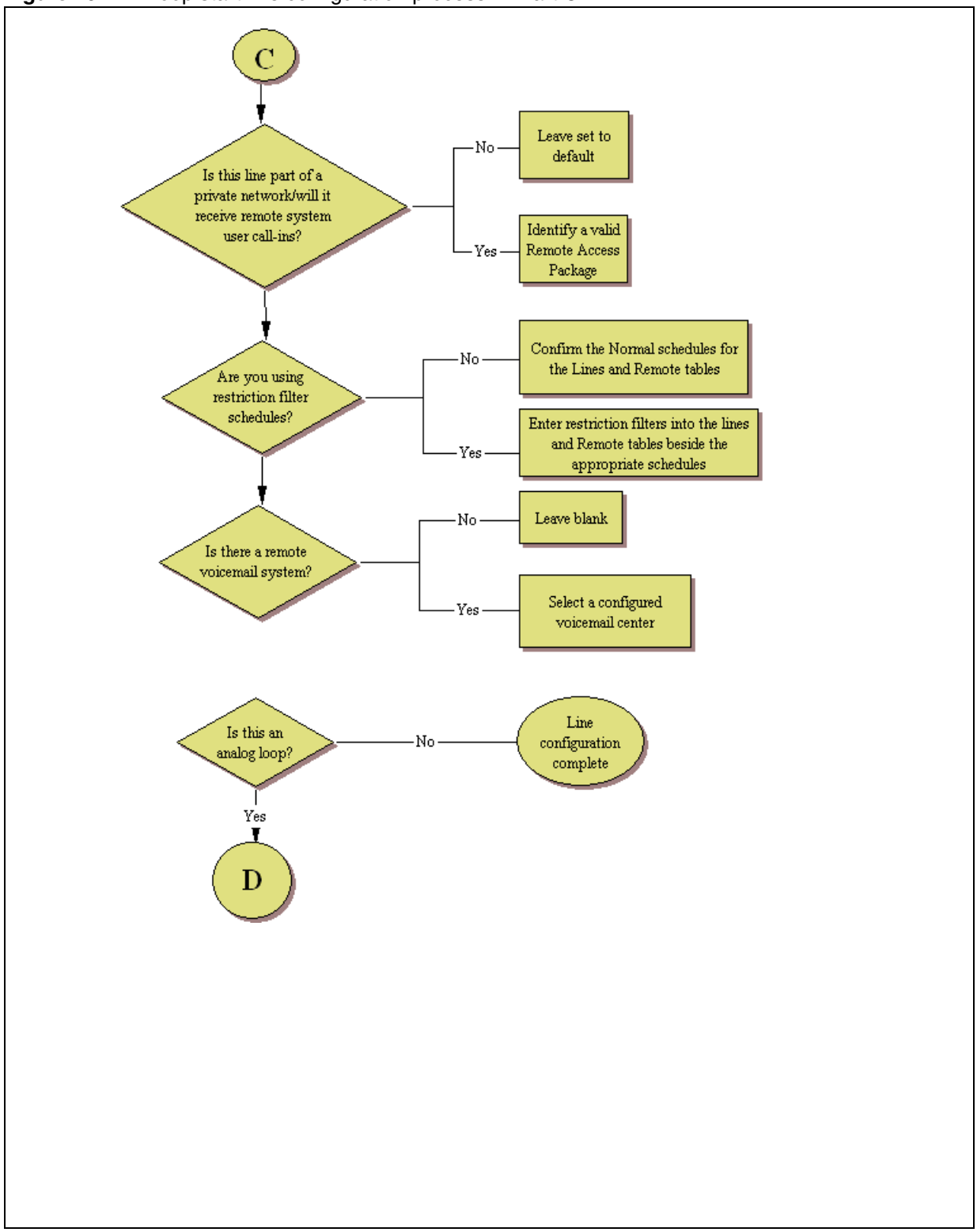


Figure 49 T1-Loop start line configuration process — Part C


C
Is this line part of a private network/will it receive remote system user call-ins?
No
Leave set to default
Yes
Identify a valid Remote Access Package
Are you using restriction filter schedules?
No
Confirm the Normal schedules for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Is there a remote voicemail system?
No
Leave blank
Yes
Select a configured voicemail center
Is this an analog loop?
No
Line configuration complete
Yes
D

Configuring digital (T1/E1) loop start lines

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

To configure digital loop start lines

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Line: Read only list shows available lines for system.
- Trunk Type: Loop.
- Name: Default name is line number, shown as part of incoming CLID.
- Control Set: If you use schedules, enter DN for telephone that controls line schedules.
- Line Type: Define as public, if the line is shared or as Private To (DN) if the line is assigned to a specific telephone, or put it in a line pool (A to O).
- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).

Under the Properties tab:

- Trunk mode: Define whether the line will detect the open switch interval (OSI) when a call is released (supervised). Note: UK profiles use Loop guarded/Loop unguarded.
- Dial mode: The line service will dictate whether this needs to be set to Pulse or Tone (DTMF) dialing.

2 Configure the trunk/line data (Preferences tab):

- Auto privacy: If you activate this feature, the line is available only to the telephone that answers the call.
- Full autohold: This allows telephones to put a line on hold if the user picks up another line or starts to dial out on another line.
- Aux. ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- Distinct rings in use: Indicates if a special ring has been assigned.
- Answer mode/Answer with DISA: If this line is used for remote call-ins, determine how you want the line to answer (automatically, or requiring more user input). If the answer mode is set to Auto, decide whether the caller will be immediately connected to the system or whether a stuttered dialtone will require the caller to enter a CoS password.
- Voice Message Center: If the system is using a remote voice mail, select the center configured with the contact number.
- Redirect to: If you want to automatically direct calls out of the system to a specific telephone, such as a headoffice answer attendant, enter that remote number here. Ensure that you include the proper routing information.

Under the Restrictions tab:

- Use remote package: If this line allows remote call-ins, ensure that you define a remote package.
- Line Restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Restrictions: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

3 Assign the lines to DNs ("Assigned DNs" on page 138)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs here. The DN record also can be used to assign lines.

- DN: Unique number
- Appearance Type: Choose Appr only or Appr&Ring if the telephone has an available button with indicator, otherwise choose Ring only. The 7000 and 7100 digital phones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting. Check with your system administrator for the system voice mail setup before changing this parameter.

4 If the lines are assigned to a line pool:

- assign the line pool to DNs ("Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300))
- also assign a target line to the DN record. ("Line Access - Line Assignment tab" and,"Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300).)

5 Suggested next steps:

- Dialing plan
  "Dialing plan: System settings" on page 267
  "Dialing plan: Public network" on page 275
  "Dialing plan: Routing and destination codes" on page 259
- Networking
  "Public networking: Setting up basic systems" on page 289
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339

Chapter 15
Configuring lines: T1-Digital Ground Start

The following describes how to configure digital Ground Start lines.

The following paths indicate where to access the Ground Start lines through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: Configure ground start lines connected to the system
• "Configuring digital ground start line features" on page 166

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured. Refer to "Trunk Module Parameters" on page 104.	
Lines are provisioned. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 50 and Figure 51 provide an overview of the line features for Ground Start lines.

Figure 50 T1-Digital Ground Start lines configuration process — Part A

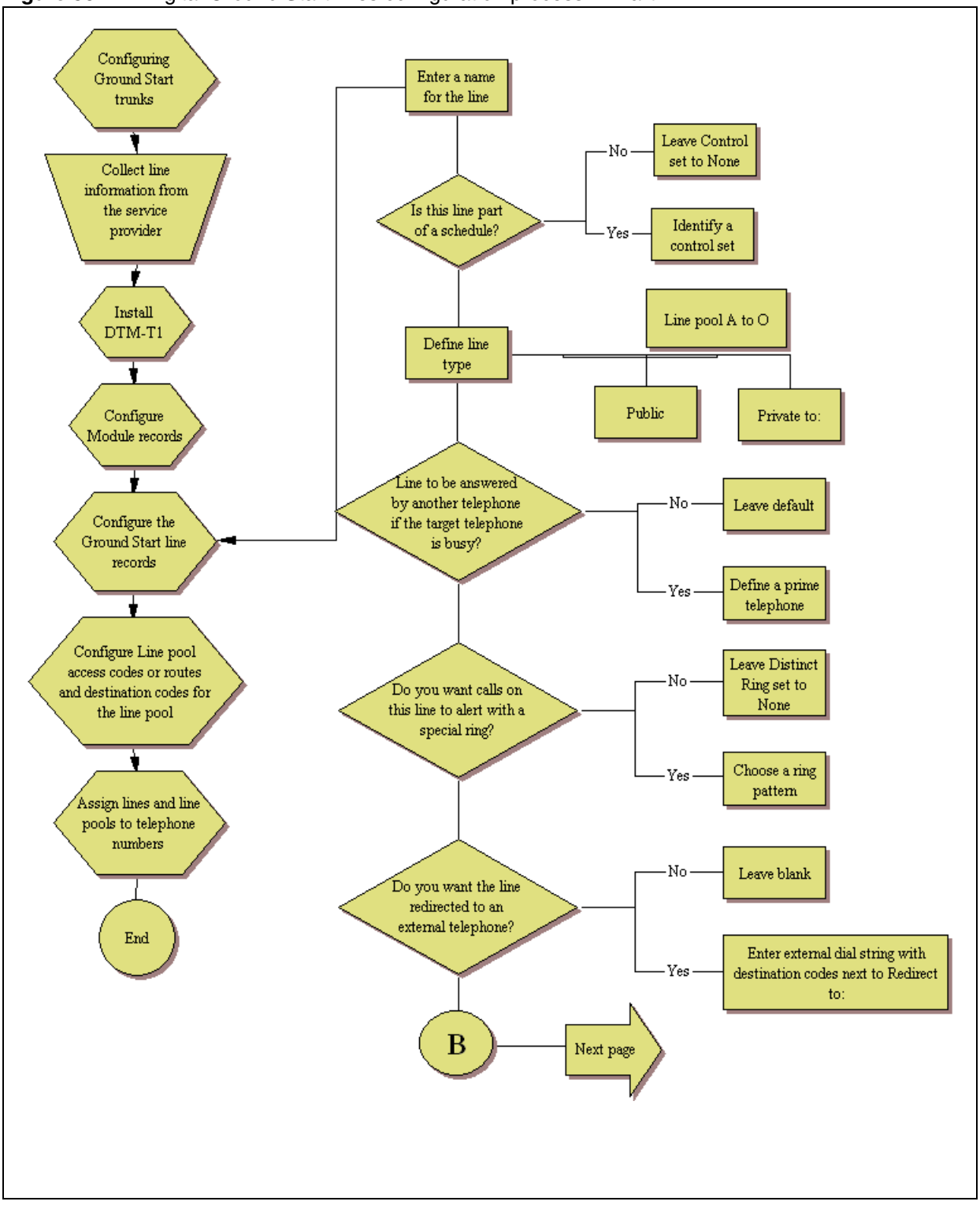
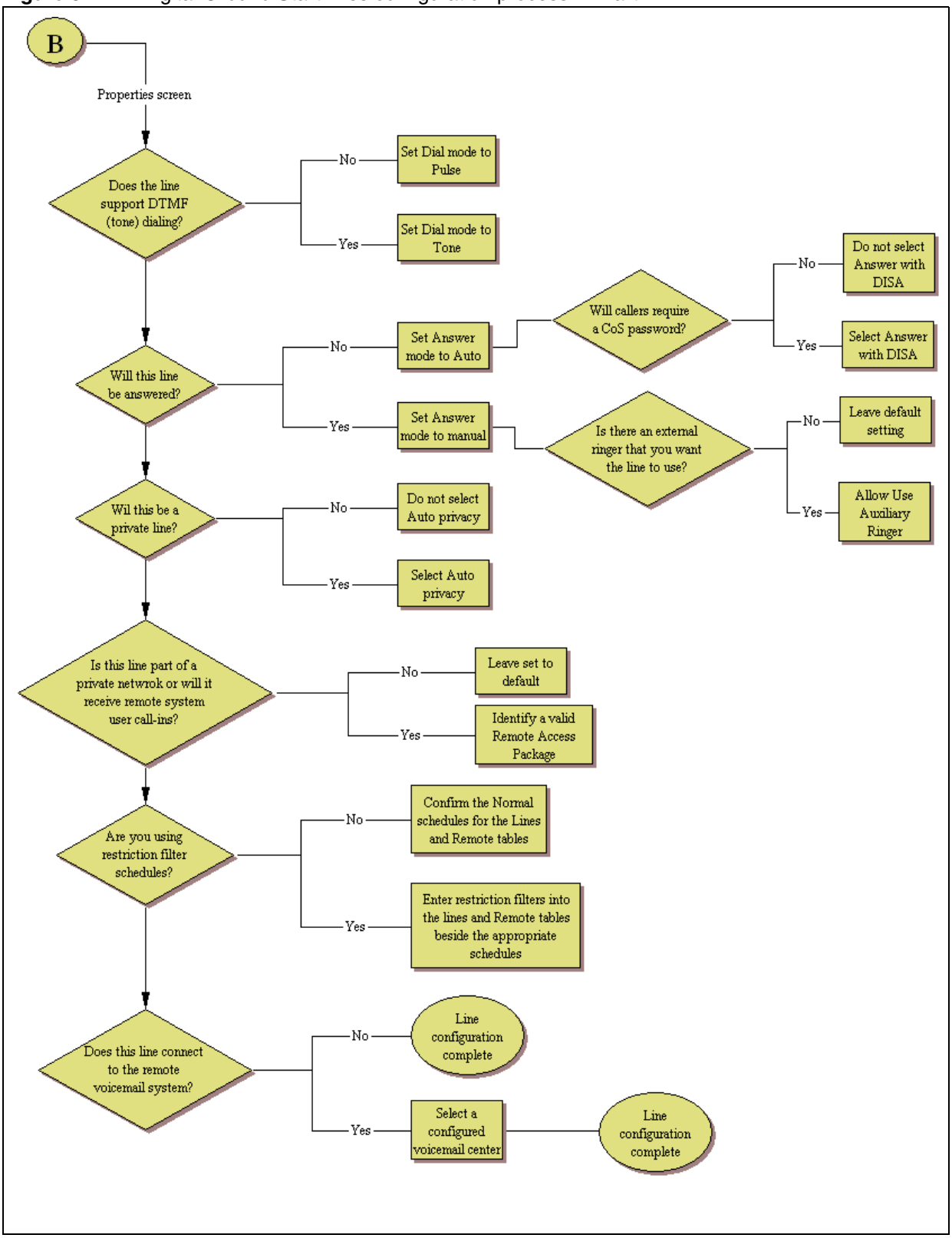

Configuring Ground Start trunks
Collect line information from the service provider
Install DTM-T1
Configure Module records
Configure the Ground Start line records
Configure Line pool access codes or routes and destination codes for the line pool
Assign lines and line pools to telephone numbers
End
Enter a name for the line
Is this line part of a schedule?
No
Leave Control set to None
Yes
Identify a control set
Define line type
Line pool A to O
Public
Private to:
Line to be answered by another telephone if the target telephone is busy?
No
Leave default
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Leave Distinct Ring set to None
Yes
Choose a ring pattern
Do you want the line redirected to an external telephone?
No
Leave blank
Yes
Enter external dial string with destination codes next to Redirect to:
B
Next page

Figure 51 T1-Digital Ground Start lines configuration process — Part B


B
Properties screen
Does the line support DTMF (tone) dialing?
No
Set Dial mode to Pulse
Yes
Set Dial mode to Tone
Will this line be answered?
No
Set Answer mode to Auto
Will callers require a CoS password?
No
Do not select Answer with DISA
Yes
Select Answer with DISA
Yes
Set Answer mode to manual
Is there an external ringer that you want the line to use?
No
Leave default setting
Yes
Allow Use Auxiliary Ringer
Wil this be a private line?
No
Do not select Auto privacy
Yes
Select Auto privacy
Is this line part of a private netwrok or will it receive remote system user call-ins?
No
Leave set to default
Yes
Identify a valid Remote Access Package
Are you using restriction filter schedules?
No
Confirm the Normal schedules for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Does this line connect to the remote voicemail system?
No
Line configuration complete
Yes
Select a configured voicemail center
Line configuration complete

Configuring digital ground start line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

To configure digital Ground Start line features

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Line: Unique number.
- Trunk type: Ground Start.
- Name: Identify the line or line function.
- Control set: Identify a DN if you are using this line with scheduling.
- Line type: Define how the line will be used. If you are using routing, ensure it is put into line pool (A to O). If you are using line pools, you must also configure target lines. ("Configuring lines: Target lines" on page 141)
- Prime set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).
- Restrictions tab: Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid package.

2 Configure the trunk/line data (Properties tab):

- Auto privacy: If you activate this feature, the line is available only to the telephone that answers the call.
- Dial mode: The line service will dictate whether this needs to be set to Pulse or Tone (DTMF) dialing.
- Answer mode/Answer with DISA: If this line is used for remote call-ins, determine how you want the line to answer (automatically, or requiring more user input). If the answer mode is set to Automatic, decide whether the caller will be immediately connected to the system or whether a stuttered dial tone will require the caller to enter a CoS password.
- Aux. ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- Redirect to: If you want to automatically direct calls out of the system to a specific telephone, such as a headoffice answer attendant, enter that remote number here. Ensure that you include the proper routing information.
- Voice Message Center: If the system is using a remote voice mail, select the center configured with the contact number.

3 Set the restriction and remote package scheduling (Restrictions tab):

- Line restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)

- Remote Packages: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

4 Assign the lines to DNs (Assigned DNs tab)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs here. The DN record also can be used to assign lines and line pools for these lines.

- Appearance Type: Choose Appr only or Appr&Ring if the telephone has an available button, otherwise choose Ring only. Model 7000 and 7100 telephones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting. Check with your system administrator for the system voice mail setup before changing this parameter.

5 Suggested next steps:

- Dialing plan
  "Dialing plan: System settings" on page 267
  "Dialing plan: Public network" on page 275
  "Dialing plan: Routing and destination codes" on page 259
- Networking
  "Public networking: Setting up basic systems" on page 289
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339

Chapter 16
Configuring lines: T1-DID

DID (Direct Inward Dial) are lines on a digital trunk module on a T1. Inbound DID lines are mapped through target lines.

The following paths indicate where to access the DID lines in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: Configure the properties for DID (Direct Inward Dial) lines

• "Configuring DID line features" on page 172

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured. Refer to "Trunk Module Parameters" on page 104.	
Lines are provisioned. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 52 and Figure 53 provide an overview of the DID line features configuration process.

Figure 52 DID line feature configuration process — Part A

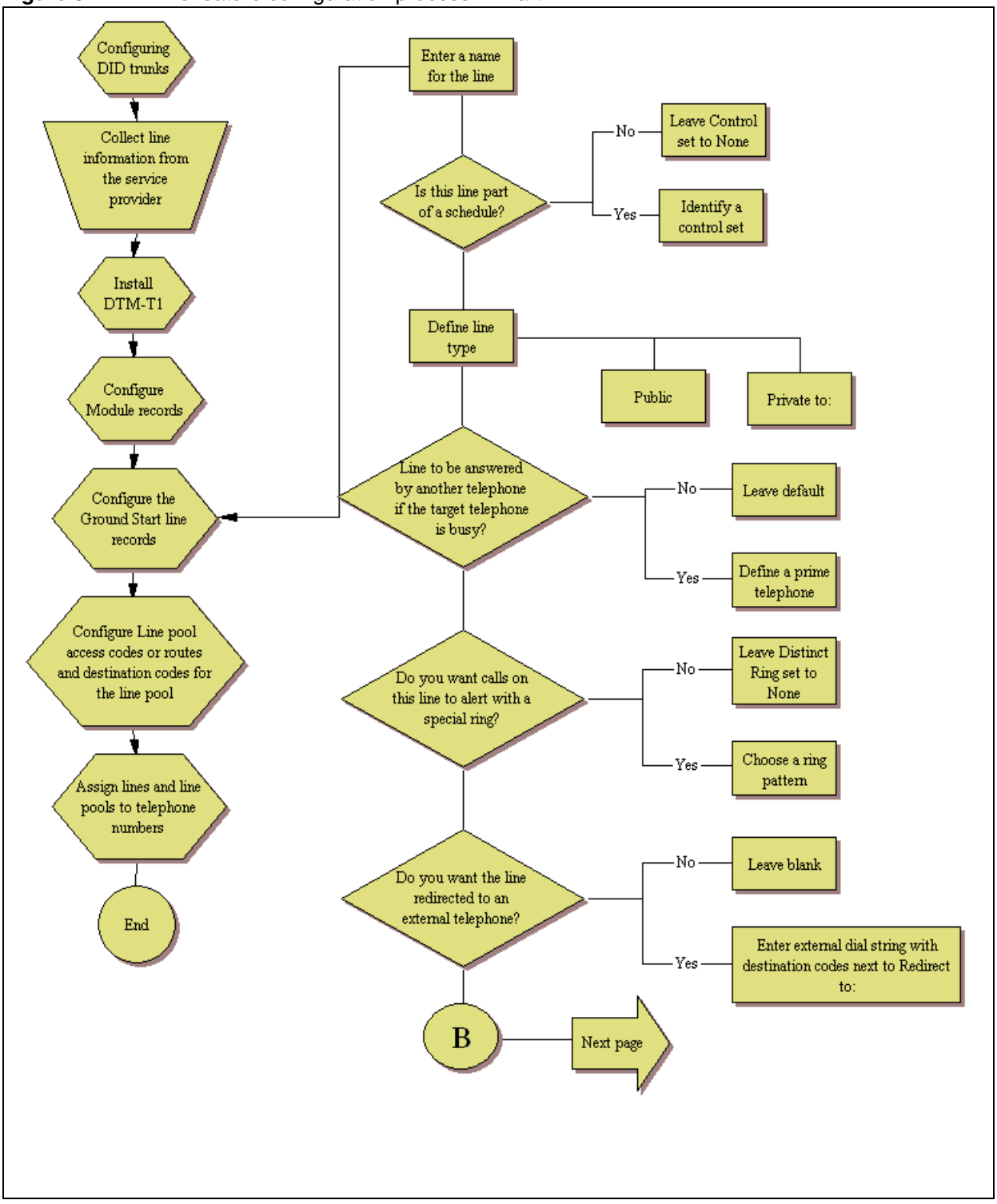
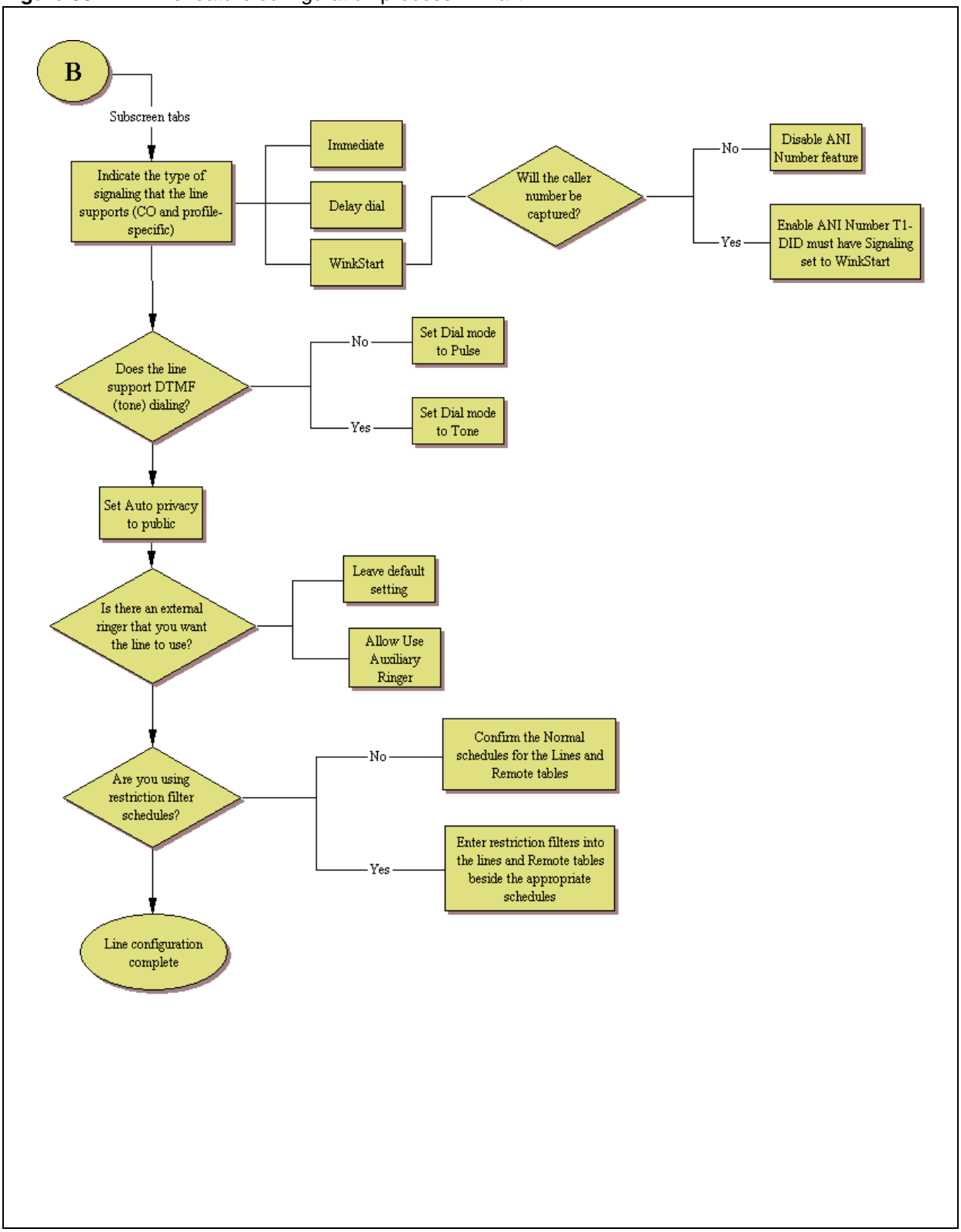

Configuring DID trunks
Collect line information from the service provider
Install DTM-T1
Configure Module records
Configure the Ground Start line records
Configure Line pool access codes or routes and destination codes for the line pool
Assign lines and line pools to telephone numbers
End
Enter a name for the line
Is this line part of a schedule?
No
Leave Control set to None
Yes
Identify a control set
Define line type
Public
Private to:
Line to be answered by another telephone if the target telephone is busy?
No
Leave default
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Leave Distinct Ring set to None
Yes
Choose a ring pattern
Do you want the line redirected to an external telephone?
No
Leave blank
Yes
Enter external dial string with destination codes next to Redirect to:
B
Next page

Figure 53 DID line feature configuration process — Part B


B
Subscreen tabs
Indicate the type of signaling that the line supports (CO and profile-specific)
Immediate
Delay dial
WinkStart
Will the caller number be captured?
No
Disable ANI Number feature
Yes
Enable ANI Number T1-DID must have Signaling set to WinkStart
Does the line support DTMF (tone) dialing?
No
Set Dial mode to Pulse
Yes
Set Dial mode to Tone
Set Auto privacy to public
Is there an external ringer that you want the line to use?
Leave default setting
Allow Use Auxiliary Ringer
Are you using restriction filter schedules?
No
Confirm the Normal schedules for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Line configuration complete

Configuring DID line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

To configure DID line features

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Trunk Type: T-1 DID
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.
- Line Type: Define as public if the line is shared, or as Private To (DN) if the line is assigned to a specific telephone.
- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, or 4).
- Use remote package: Not applicable.

2 Configure the trunk/line data (Properties tab):

- Dial mode: The line service will dictate whether this needs to be set to Pulse or Tone (DTMF) dialing.
- Loss package: Define the appropriate loss/gain and impedance settings for the line
- Signaling: Match this choice with the information supplied by the service provider.
- Link at CO: Enable if provider switch provides alternative line when F71 is invoked for an outgoing call
- Line Tuning Digit:

3 Configure the Preferences tab:

- Auto privacy: If you activate this feature, the line is available only to the telephone that answers the call.
- Aux. ringer: Use if your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- ANI number: Enable if the caller number is to be logged. For T1 lines, this only appears if Signaling is set to WinkStart.
- Distinct rings: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).
- Voice message center: If the system is using a remote voice mail, select the center configured with the contact number.
- Redirect to: If you want to automatically direct calls out of the system to a specific telephone, such as a headoffice answer attendant, enter that remote number here. Ensure that you include the proper routing information.

4 Set the restriction and remote package scheduling (Restrictions tab):

- Line restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Restrictions: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

5 Assign the lines to DNs (Assigned DNs tab) (applicable to manual answer only)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs, here. The DN record also can be used to assign lines and line pools for these lines.

- Appearance type: Choose Appear or Appear and ring if the telephone has an available button, otherwise choose Ring Only. Model 7000 and 7100 telephones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting.

  Check with your system administrator for the system voice mail setup before changing this parameter.

6 Suggested next steps:

- Dialing plan
  "Dialing plan: System settings" on page 267
  "Dialing plan: Public network" on page 275
  "Dialing plan: Routing and destination codes" on page 259
- Networking
  "Public networking: Setting up basic systems" on page 289
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339

Chapter 17
Configuring lines: DASS2 lines

DASS2 trunks are specific to the UK protocol.

The following paths indicate where to access the DASS2 trunks in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset Interface: ****CONFIG > Lines**

Task: configure DPNSS lines connected to the system

- "Configuring DASS2 line features" on page 177
- Also refer to "Private networking: DPNSS network services (UK only)" on page 331

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured. Refer to "Trunk Module Parameters" on page 104.	
Lines are provisioned. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 54 and Figure 55 provide an overview of the DASS2 line feature configuration.

Figure 54 DASS2 line feature configuration process — Part A

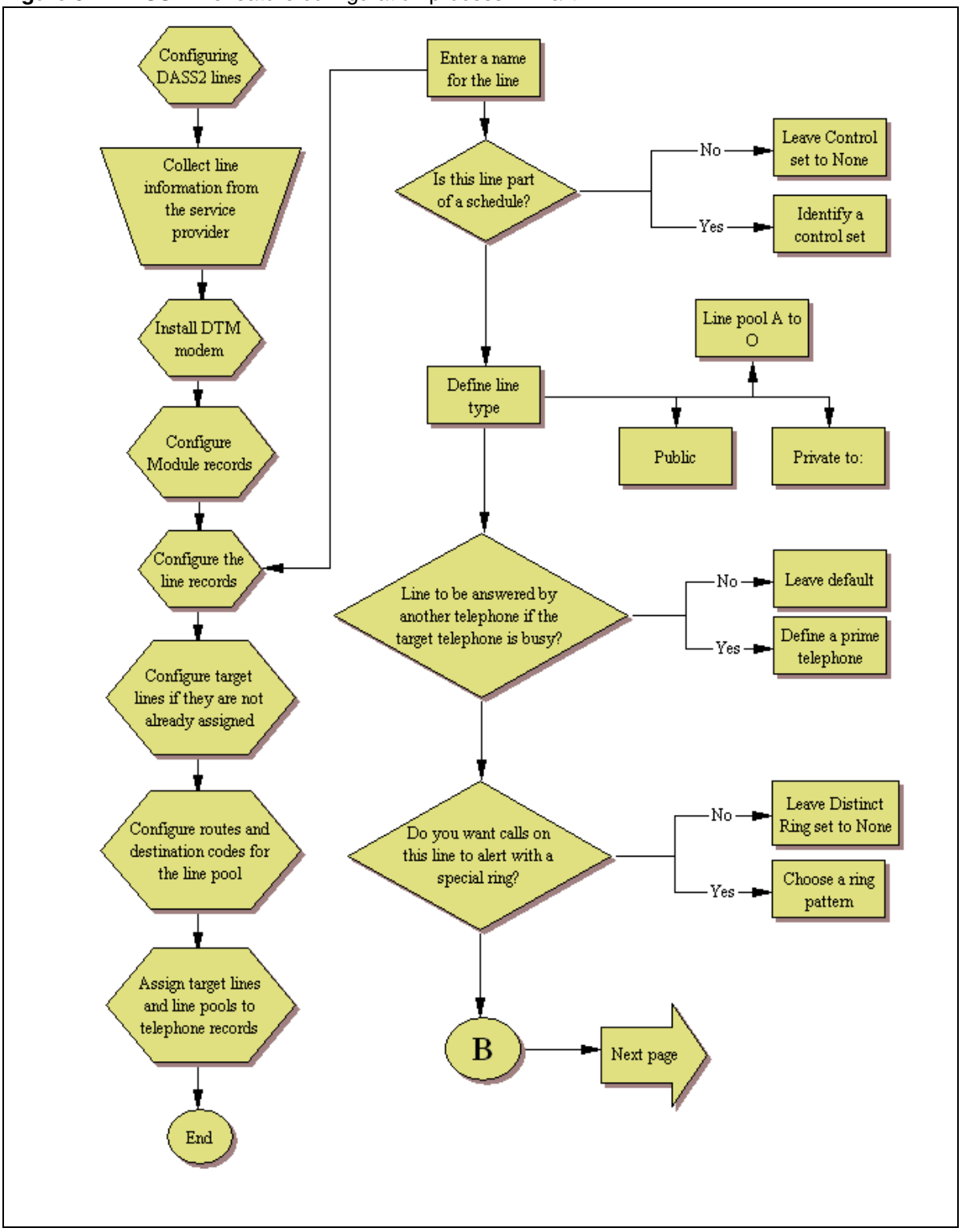
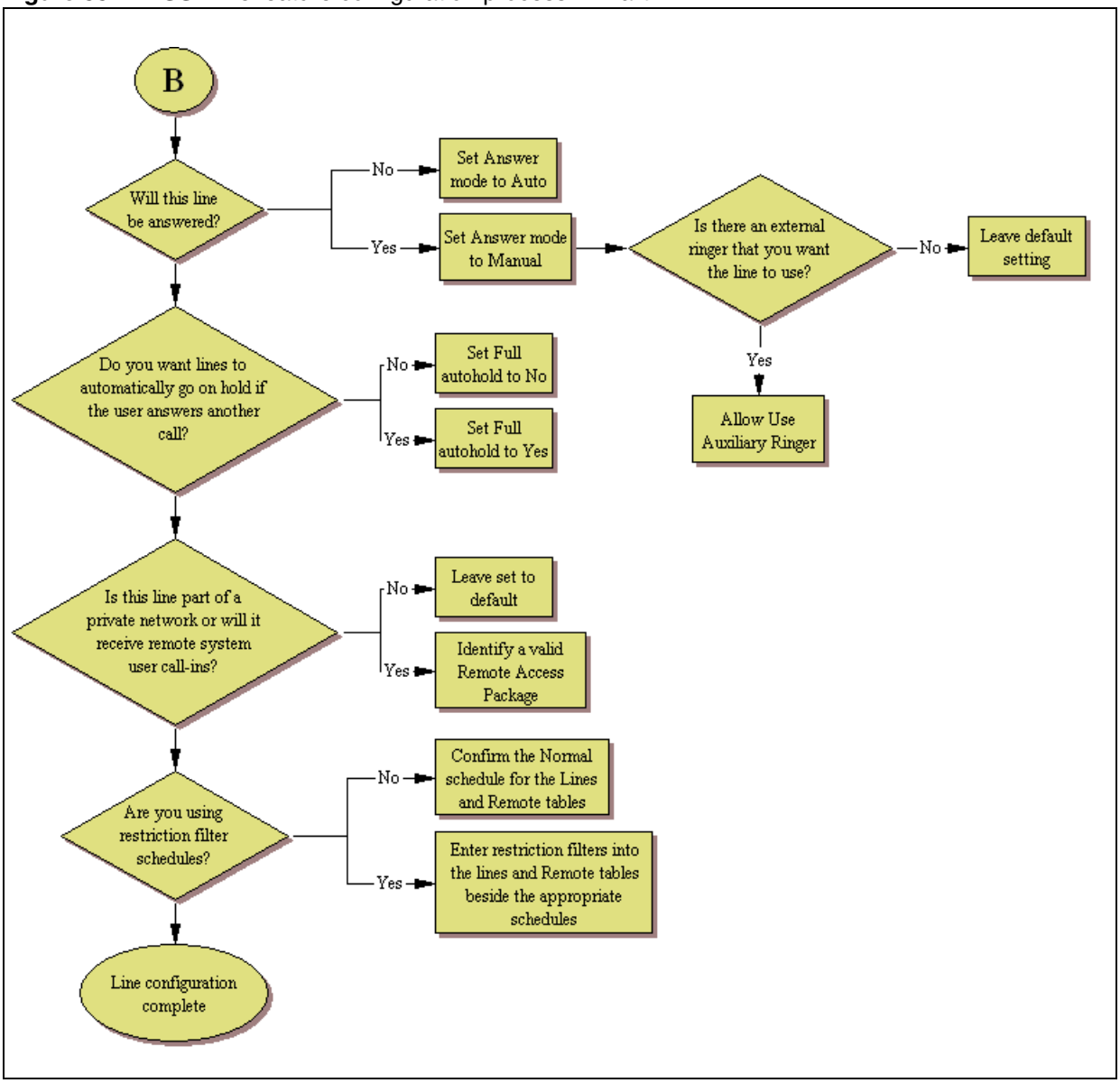

Configuring DASS2 lines
Collect line information from the service provider
Install DTM modem
Configure Module records
Configure the line records
Configure target lines if they are not already assigned
Configure routes and destination codes for the line pool
Assign target lines and line pools to telephone records
End
Enter a name for the line
Is this line part of a schedule?
No
Leave Control set to None
Yes
Identify a control set
Define line type
Line pool A to O
Public
Private to:
Line to be answered by another telephone if the target telephone is busy?
No
Leave default
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Leave Distinct Ring set to None
Yes
Choose a ring pattern
B
Next page

Figure 55 DASS2 line feature configuration process — Part B


B
Will this line be answered?
No
Set Answer mode to Auto
Yes
Set Answer mode to Manual
Is there an external ringer that you want the line to use?
No
Leave default setting
Yes
Allow Use Auxiliary Ringer
Do you want lines to automatically go on hold if the user answers another call?
No
Set Full autohold to No
Yes
Set Full autohold to Yes
Is this line part of a private network or will it receive remote system user call-ins?
No
Leave set to default
Yes
Identify a valid Remote Access Package
Are you using restriction filter schedules?
No
Confirm the Normal schedule for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Line configuration complete

Configuring DASS2 line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Trunk type: DASS2
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.

- Line type: Define how the line will be used. If you are using routing, ensure it is put into line pool (A to O).
- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4 or None).
- Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid package.

2 Configure the trunk/line data (Properties tab):

- Answer mode: If this line is used for remote call-ins, determine how you want the line to answer (automatically, or requiring more user input).
- Use auxiliary ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- Full autohold: This allows telephones to put a line on hold if the user picks up another line or starts to dial out on another line.
- Voice Message Center: If the system is using a remote voice mail, select the center configured with the contact number.

3 Set the restriction and remote package scheduling (Restrictions tab):

- Line restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Packages: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

4 Assign the lines to DNs (Assigned DNs tab)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs, here. The DN record also can be used to assign lines and line pools for these lines.

- Appearance type: Choose Appr or Appr&ring if the telephone has an available button, otherwise choose Ring only. Model 7000 and 7100 telephones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting. Check with your system administrator for the system voice mail setup before changing this parameter.

5 Suggested next steps:

- Dialing plan

"Dialing plan: System settings" on page 267
"Dialing plan: Public network" on page 275
"Dialing plan: Private network settings" on page 281
"Dialing plan: Routing and destination codes" on page 259

- Networking
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339
  "Private networking: DPNSS network services (UK only)" on page 331
  "Private networking: MCDN over PRI and VoIP" on page 297

Chapter 18
Configuring lines: DPNSS lines

DPNSS trunks are specific to the UK protocol.

The following paths indicate where to access the DPNSS trunks in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Task: configure DPNSS lines connected to the system

- "Configuring DPNSS line features" on page 183
- Also refer to "Private networking: DPNSS network services (UK only)" on page 331

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured. Refer to "Trunk Module Parameters" on page 104.	
Lines are provisioned. Refer to "Provisioning module lines/loops" on page 112.	

Process map

Figure 56 and Figure 57 provide an overview of the DPNSS line feature configuration process.

Figure 56 DPNSS line feature configuration process — Part A

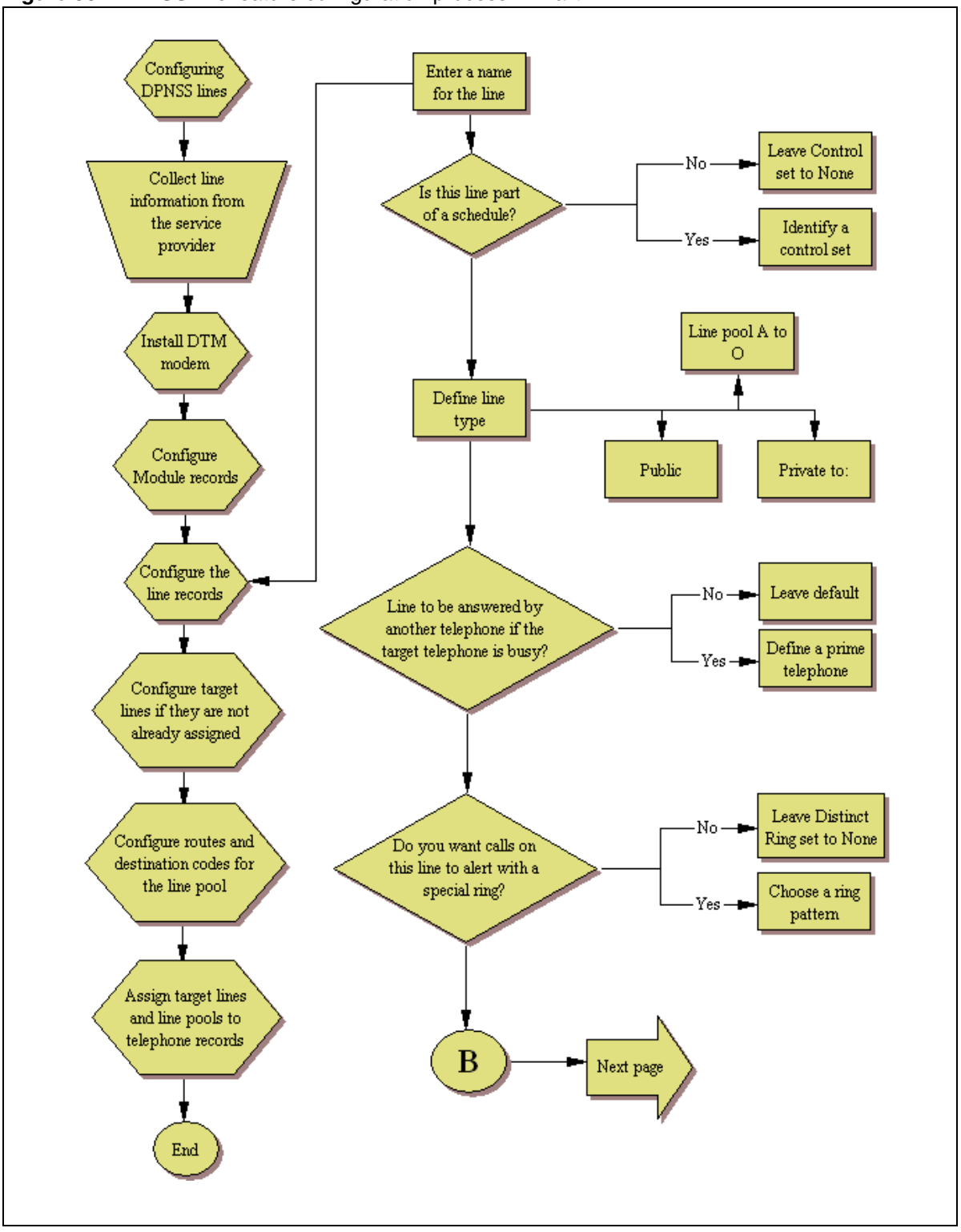
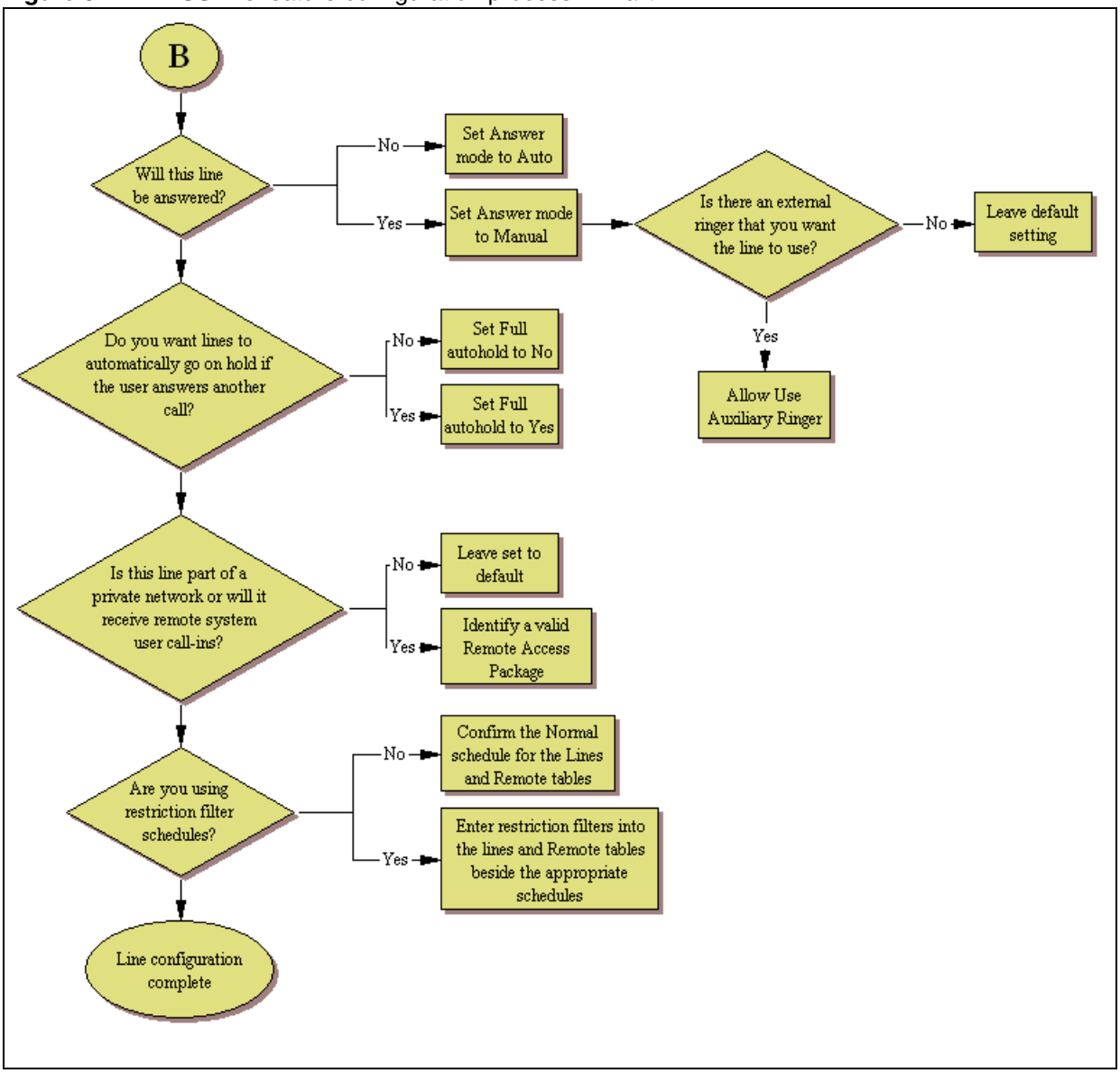

Configuring DPNSS lines
Collect line information from the service provider
Install DTM modem
Configure Module records
Configure the line records
Configure target lines if they are not already assigned
Configure routes and destination codes for the line pool
Assign target lines and line pools to telephone records
End
Enter a name for the line
Is this line part of a schedule?
No
Leave Control set to None
Yes
Identify a control set
Define line type
Line pool A to O
Public
Private to:
Line to be answered by another telephone if the target telephone is busy?
No
Leave default
Yes
Define a prime telephone
Do you want calls on this line to alert with a special ring?
No
Leave Distinct Ring set to None
Yes
Choose a ring pattern
B
Next page

Figure 57 DPNSS line feature configuration process — Part B


B
Will this line be answered?
No
Set Answer mode to Auto
Yes
Set Answer mode to Manual
Is there an external ringer that you want the line to use?
No
Leave default setting
Yes
Allow Use Auxiliary Ringer
Do you want lines to automatically go on hold if the user answers another call?
No
Set Full autohold to No
Yes
Set Full autohold to Yes
Is this line part of a private network or will it receive remote system user call-ins?
No
Leave set to default
Yes
Identify a valid Remote Access Package
Are you using restriction filter schedules?
No
Confirm the Normal schedule for the Lines and Remote tables
Yes
Enter restriction filters into the lines and Remote tables beside the appropriate schedules
Line configuration complete

Configuring DPNSS line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Trunk type: DPNSS
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.
- Line type: Define how the line will be used. If you are using routing, ensure it is put into line pool (A to O).

- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received #: Not applicable.
- Distinct ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4 or None).
- Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid package.

2 Configure the trunk/line data (Properties tab):

- Answer mode: If this line is used for remote call-ins, determine how you want the line to answer (automatically, or requiring more user input).
- Use auxiliary ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- Full autohold: This allows telephones to put a line on hold if the user picks up another line or starts to dial out on another line.
- Voice Message Center: If the system is using a remote voice mail, select the center configured with the contact number.

3 Set the restriction and remote package scheduling (Restrictions tab):

- Line restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Packages: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

4 Assign the lines to DNs (Assigned DNs tab)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs, here. The DN record also can be used to assign lines and line pools for these lines.

- Appearance type: Choose Appr or Appr&ring if the telephone has an available button, otherwise choose Ring only. Model 7000 and 7100 telephones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting. Check with your system administrator for the system voice mail setup before changing this parameter.

5 Suggested next steps:

- Dialing plan

"Dialing plan: System settings" on page 267
"Dialing plan: Public network" on page 275
"Dialing plan: Private network settings" on page 281
"Dialing plan: Routing and destination codes" on page 259

- Networking
  "Public networking: Tandem calls from private node" on page 293
  "Private networking: Using destination codes" on page 339
  "Private networking: DPNSS network services (UK only)" on page 331
  "Private networking: MCDN over PRI and VoIP" on page 297

Chapter 19
BRI ISDN: BRI loop properties

The Loops tables display settings for installed BRI modules.

The BCM50b, BCM50ba, and BCM50be models include an integrated BRI module which equips the system with two T-loops. The T-loops can be changed to S-loops depending on your system requirements. The default loops are 301 and 302.

Physical lines 061-064 are always assigned to the BRI cNIC.

Refer to the *BCM50 2.0 Installation and Maintenance Guide* (NN40020-302) for more information on the BCM50 integrated BRI models.

The following paths indicate where to access the loops table for BRI modules in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Loops**
- Telset interface: ****CONFIG > Hardware > Module > TrunkMod > BRI - X > Loop XXX**

This panel contains the following tab:

- Loops - provides configuration for general loop settings.

Click one of the following links to connect with the type of information you want to view:

Panel tabs	Tasks
"Configure loop type and general parameters" on page 188	ONN blocking
"T-loop general settings" on page 189	"Provisioning module lines/loops" on page 112 "Configuring lines" on page 129 "Configuring lines: T1-Loop start" on page 157
"T-loop SPIDS and network DNs" on page 190	"BRI ISDN: BRI T-loops" on page 195
"S-loops assigned DNs" on page 193	"Programming BRI S-loops, lines, and ISDN devices" on page 201 "DN records parameters" in the *Device Configuration Guide* (NN40020-300)
"T-loops D-packet service" on page 192	

Click the navigation tree heading to access general information about user management.

You can define BRI loops as either T-loops, for connecting to ISDN trunks, or S-loops, for connecting to internal ISDN equipment. Both types of loops are displayed in the top frame in the Loop Parameters panel. In the bottom frame, the settings displayed are specific to each type of loop.

Configure loop type and general parameters

The Loops table displays the BRI loops for an installed module and the settings that are common to both T-loops and S-loops. Figure 58 illustrates the Loops table.

Figure 58 Loops table

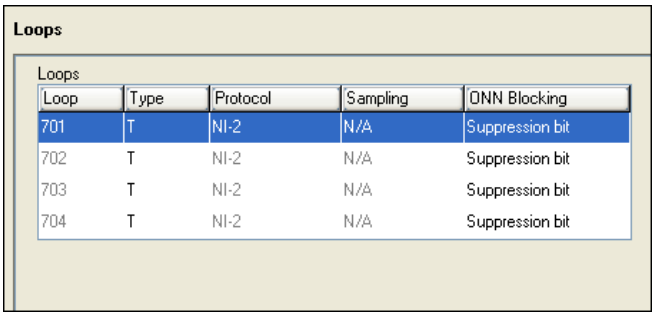


Table 31 describes the fields found on the Loop main panel.

Table 31 Loops main panel (Sheet 1 of 2)

Attribute	Value	Description
Loop	<X01-X04>	Each BRI module supports four loops (eight lines for T-loop programming).
Type	T S	This setting defines whether the loop supports trunks (T-loop) or device connections (S-loop). **Note**: This variable may be different for different market profiles.
Protocol	Euro QSIG NI-2	Select the appropriate ISDN protocol. The values displayed depend on both the market profile and software keycodes. Euro - ETSI ISDN standard QSIG - also an ETSI standard. Only appears if the ETSI QSIG keycode is loaded. NI-2
Sampling (S-loops only)	Adaptive Fixed N/A	Select a sampling rate for the S-loop. Fixed: two or more S-interface devices use the loop, and the length of the loop is less than 200 m (650 ft.). Adaptive: two or more S-interface devices use the loop, and the length of the loop is greater than 200 m (650 ft.). If one device is using the loop, the length of the loop can be a maximum of 1000 m (3230 ft)
ONN blocking	Suppression bit Service code	Set the Outgoing Name and Number (ONN) Blocking. When you activate ONN, a user can press **FEATURE 819** to block the outgoing name and number on a per call basis. **Programming note**: Ensure that all telephones that have this feature available are assigned valid OLI numbers. Refer to “Programming outgoing number display (OLI)” on page 209.

Table 31 Loops main panel (Sheet 2 of 2)

Attribute	Value	Description
ONN blocking		**Suppression bit:** the system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call. **Service code:** VSC digits are dialed out before the called number to activate ONN at the central office. These codes are supplied by your service provider for the lines. Refer to "ONN Blocking codes (North American systems)" in the *Device Configuration Guide* (NN40020-300). PRI lines have only one code, so do not require specific configuration.

T-loop general settings

The Settings tab allows you to define loop characteristics. Note that not all of these settings are required in all BRI markets. Figure 59 illustrates the Settings tab.

Figure 59 Settings subpanel (T loops)

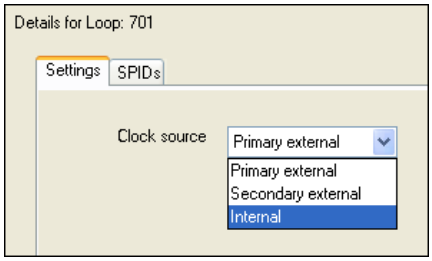


Table 32 describes the fields on this panel.

Table 32 Details for Loop (Sheet 1 of 2)

Attribute	Value	Description
Clock source	Primary External Secondary External Internal	Primary External - uses clock from PSTN Secondary External - used if system has more than one Loop Internal - uses clock on BCM
Overlap: receiving	<check box>	Supports target lines in markets which use Overlap receiving signaling on the BRI trunks. Overlap receiving must be configured for each BRI loop.
Overlap: length	<0-15>	Set the local number length for loops to interfaces that receive overlap rather than enbloc digits. This number is the total length of the called party number received. This number is used to calculate the number of leading digits that need to be removed by the system.

Table 32 Details for Loop (Sheet 2 of 2)

	Note: This parameter appears only when Overlap receiving is enabled. Example: Public received number = 4502303 Target line received numbers = 303 Local number length = 7 Public received number length = 3 Thus the first four digits are deleted by the system.	
Send Name Display (ETSI QSIG only)	<check box>	If the switch allows outgoing name display, select the check box.

T-loop SPIDS and network DNs

These settings are only available for systems running a North American profile. SPID numbers are supplied by the ISDN service provider. Also refer to "ISDN overview" on page 535.

Figure 60 illustrates the SPIDs tab.

Figure 60 SPIDs and network DNs (T-loops, North America only)

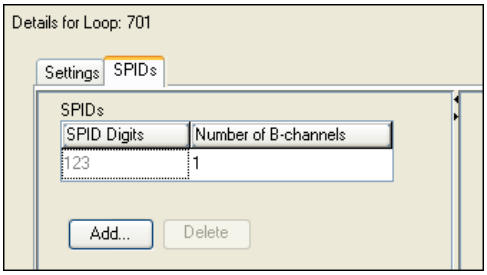


Table 33 defines the fields on the SPIDs tab and indicates the lines.

Table 33 Loop settings (Sheet 1 of 2)

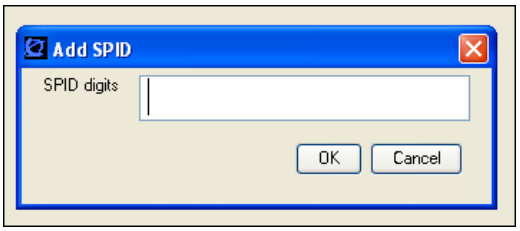
Attribute	Value	Description
SPIDS table		
SPID Digits	<digits>	Supplied by your service provider. System running with North American country profiles support additional BRI services offered by ISDN service providers and defined by network service profile identifiers (SPID). The SPID allows you to enter a network connection that provides a path for voice or data services
Number of B-channels	1, 2	North American BRI loops can support two B-channels. The SPID may be the same or different for the channels.
Actions		
Add (SPID digits)	1. Select the appropriate SPID (1 or 2) 2. Click **Add**.  3. Enter the SPID digits supplied by your ISDN service provider. 4. Click **OK**. 5. On the table, click the Number of B-channels field beside the number you entered. 6. Choose the number of B-channels allowed for this SPID.	
Delete	1. Select the SPID that you want to delete. 2. Click **Delete**. 3. Click **OK**.	
Network DNs table		
DN	<system DN>	This ISDN DN acts as the contact point for the loop to the system.
Call Type	Voice Data Both	Defines the type of calls supported on the loop.

Table 33 Loop settings (Sheet 2 of 2)

Attribute	Value	Description
Actions		
Add	1. Select the appropriate SPID (1 or 2) 2. Under the Details for SPID table, click **Add**. 3. Enter a network DN. 4. Click **OK**. 5. On the table, click in the Call Type field beside the DN you entered. 6. Choose the call type for the DN.	
Delete	1. Select the SPID that you want to delete. 2. Click **Delete**. 3. Click **OK**.	

T-loops D-packet service

The D-Packet Service panel is the second tab of the loops panels.

Note: D-Packet service is only available if your service provider provides this Capability

This panel enables you to configure D-Packet Service to T-loops. You must have both T-loops and S-loops configured on the same module to allow this feature.

Figure 61 illustrates the D-Packet Service panel.

Figure 61 D-packet service (T-loops)

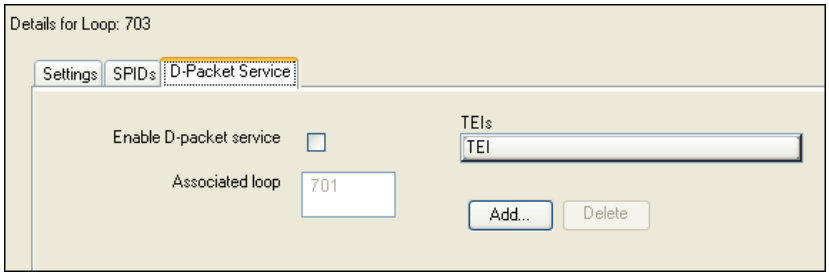
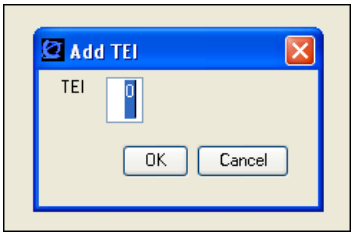


Table 34 describes each section on the D-Packet Service panel.

Table 34 D-packet settings

Attribute	Value	Description
Associated loop	X01-X04	T-loop: This is the loop on the BRI module that is configured as the T-loop and is connected to the external trunk. S-loop: This is the loop on the BRI module where the device is connected.
Enabled D-packet Service	<check box>	Enable this service, only if you are installing devices that require this type of service.
TEI	<digits>	These entries identify up to eight terminal identifiers for the devices assigned to the S-loops. Your BRI service provider supplies these numbers, if they are required.
Actions		
Add	1. In the top frame, click the loop where you want to define D-Packet Service. 2. In the bottom frame, Ensure Enable D-packet service check box is selected. 3. In the Associated loop field, enter a defined S-loop. 4. Under the TEIs table, click **Add**.  5. Enter a TEI. 6. Click **OK**. 7. Repeat for all the TEIs you want to assign.	
Delete	1. In the top frame, click the loop where you want to delete TEI assignments. 2. In the bottom frame, click the TEI you want to delete. 3. Click **Delete**. 4. Click **OK**.	

S-loops assigned DNs

The Details for Loop panel for S-loops allows you to view which device records are assigned to a loop, and to add or delete a record from the loop.

Figure 62 illustrates the Details for Loop panel.

Figure 62 Assigned DNs (S-loops)

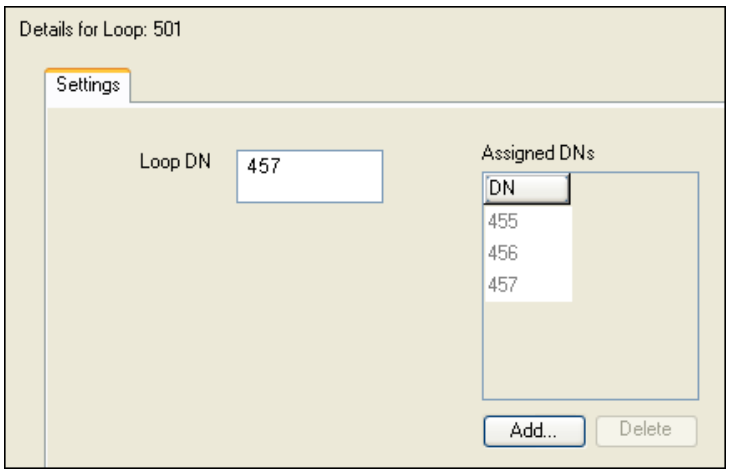


Table 35 defines the fields on the Details for Loop panel.

Table 35 Loop settings

Attribute	Value	Description
Loop DN	<system DN>	Control DN for the loop. This DN must be on the Assigned DNs list.
Assigned DNs table		
DN	<system DN>	ISDN assigned to the loop (up to eight devices)
Actions		
Add	1. In the top frame, click the loop where you want to add DN records. 2. In the bottom frame, click **Add**. 3. Enter the DN record number. 4. Click **OK**. 5. Repeat for all the DN records you want to assign.	
Delete	1. In the top frame, click the loop where you want to delete DN record assignments. 2. In the bottom frame, click the DN record you want to delete. 3. Click **Delete**. 4. Click **OK**.	

Chapter 20
BRI ISDN: BRI T-loops

BRI modules support both trunk and station (telephone) services.

The following describes the process for configuring trunk (T) loops.

Task: Configure BRI T-loops
Configuring BRI T-loop parameters on page 197

Prerequisites

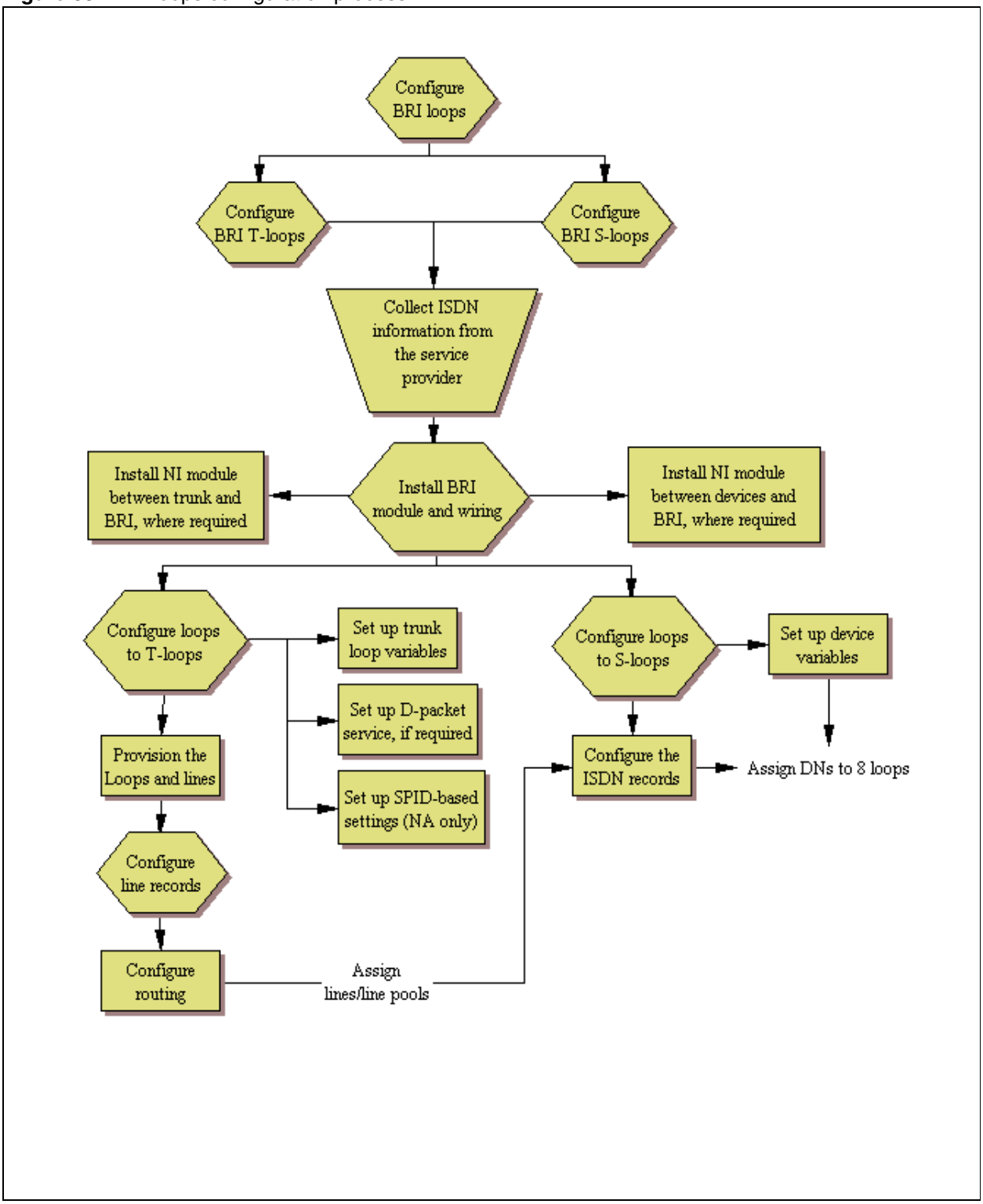
Complete the following prerequisites checklist before configuring the modules.

Ensure that system hardware is installed and operating correctly.	
Obtain all relevant central office/service provider information for the loops.	
BRI module is installed and operating (LEDs are correct).	

Process overview

Figure 63 shows the process for configuring BRI loops.

Figure 63 BRI loops configuration process


Configure BRI loops
Configure BRI T-loops
Configure BRI S-loops
Collect ISDN information from the service provider
Install NI module between trunk and BRI, where required
Install BRI module and wiring
Install NI module between devices and BRI, where required
Configure loops to T-loops
Set up trunk loop variables
Set up D-packet service, if required
Set up SPID-based settings (NA only)
Provision the Loops and lines
Configure line records
Configure routing
Assign lines/line pools
Configure loops to S-loops
Set up device variables
Configure the ISDN records
Assign DNs to 8 loops

Configuring BRI T-loop parameters

To configure BRI T-loop parameters

1 Identify the loop as a T-loop (refer to "Configure loop type and general parameters" on page 188).

- Protocol (ETSI and ETSI-QSIG loops, only)
- ONN block state
- Overlap receiving
- Overlap length
- Send name display (ETSI-QSIG only)

2 Enter the details for the loop (refer to "T-loop SPIDS and network DNs" on page 190).

North American systems, only:

- SPID
- B-channel
- Network DN
- Call type

ETSI and ETSI-QSIG T-loops (UK profile)

- Clock source

3 If applicable, configure D-packet service for the loop (refer to "T-loops D-packet service" on page 192).

4 Provision the loop and the loop lines (refer to "Provisioning module lines/loops" on page 112).

5 Program the BRI lines (refer to "Configuring BRI lines" on page 197). If the lines are set to auto-answer, put the lines into line pools (A to O) and configure target lines.

6 Assign the lines/line pools and target lines to the telephones. Refer to "Line Access - Line Assignment tab" and "Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300).

Configuring BRI lines

There are two lines for every ISDN BRI loop that is designated as a T-loop. Unlike PRI lines, these lines can be set to either manual or automatic answer when using for remote call-ins.

The following paths indicate where to access the line configuration menu through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines > Active Physical Lines, Inactive Lines, All Lines**
- Telset interface: ****CONFIG > Lines**

Prior programming:

BRI module: Installed and configured. Refer to "Trunk Module Parameters" on page 104.	
BRI loops are configured as T loops. Refer to "Configuring BRI T-loop parameters" on page 197.	
BRI loop lines are provisioned. Refer to "Provisioning module lines/ loops" on page 112.	

Configuring provisioned BRI line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

To configure provisioned BRI line features

1 Confirm or change the settings on the Trunk/Line Data main panel:

- Trunk Type: BRI-ST (determined by profile and type of BRI module)
- Name: Identify the line or line function.
- Control Set: Identify a DN if you are using this line with scheduling.
- Line Type: Define how the line will be used. If you are using routing, ensure it is put into line pool (A to O).
- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable.
- Priv. Received#: Not applicable.
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, or 4).
- Subpanel, under Restrictions tab: Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid package.

2 Configure the trunk/line data (Properties tab):

- Auto privacy: If you activate this feature, the line is available only to the telephone that answers the call.
- Answer mode/Answer with DISA: If this line is used for remote call-ins, determine how you want the line to answer (automatically, or requiring more user input). If the answer mode is set to Automatic, decide whether the caller will be immediately connected to the system or whether a stuttered dial tone will require the caller to enter a CoS password.
- Aux. ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.
- Full autohold: This allows telephones to put a line on hold if the user picks up another line or starts to dial out on another line.
- Voice Message Center: If the system is using a remote voice mail, select the center configured with the contact number.

3 Set the restriction and remote package scheduling (Restrictions tab):

- Line restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Packages: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of (incoming calls from remote users or private networks)

4 Assign the lines to DNs (Assigned DNs tab)

If you have configured the DNs and know to which telephones the line needs to be assigned, you can enter those DNs, here. The DN record also can be used to assign lines and line pools for these lines.

- Appearance Type: Choose Appr only or Appr&Ring if the telephone has an available button, otherwise choose Ring only. Model 7000 and 7100 telephones have no programmable buttons, so this must be set to Ring only. (Model 7000 phones, supported in Europe only.)
- VMsg set: When activated, an indicator on the telephone appears when a message from a remote voice-mail system is waiting.

  Check with your system administrator for the system voice mail setup before changing this parameter.

Chapter 21
Programming BRI S-loops, lines, and ISDN devices

BRI modules support both trunk and station (telephone) services. The following describes the process for configuring station/device (S) loops, which support devices that use an ISDN interface. You can assign a single device to a loop, or multiple devices connected through an NT-1 interface.

The following paths indicate where to configure loops through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Loops**
- Telset interface: ****CONFIG > Hardware > Module > TrunkMod > BRI - X > Loop XXX**

Task: Configure BRI S-loops

- "Setting BRI properties for ISDN device connections" on page 201
- "DN records: ISDN devices" on page 202

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

Ensure that system hardware is installed and operating correctly.	
Obtain all relevant central office/service provider information for the loops.	
BRI module is installed and operating (LEDs are correct).	
Wiring is complete for ISDN device configuration.	

Setting BRI properties for ISDN device connections

BRI S-loops support devices that use an ISDN interface. See "ISDN overview" on page 535. You can assign a single device to a loop, or multiple devices connected through an NT-1 interface.

- You can assign a maximum of eight devices to a loop.
- Any device can only be configured to one loop.
- S-loops do not supply any voltage for ISDN devices requiring power, such as video cameras. Voltage for these devices must be supplied by an external source on the S-loop.

For detailed descriptions of the BRI module fields, refer to "BRI ISDN: BRI loop properties" on page 187.

To set BRI properties for ISDN device connections

1 On the top panel, identify the loop as an S-loop. Refer to "Configure loop type and general parameters" on page 188.

- Sampling
- ONN block state

2 On the bottom panel, identify which ISDN DNs to associate to the loop ("S-loops assigned DNs" on page 193) (Default DNs: 597-694; additional DNs: 565-597, change type to ISDN):

- Assigned DNs
- Loop DN (must be on the Assigned DN list). If you set this field to None, unanswered calls are dropped. If the field is left blank, Assigned DNs make and receive data calls.

3 Configure the ISDN DN records for the device(s) assigned to the loop. Refer to "Configuring an ISDN telephone DN record" on page 204.

DN records: ISDN devices

ISDN telephones and devices have a limited feature set. They do not have programmable buttons or user preferences, and do not support call forward features. However, you can assign Answer DNs and some capabilities features.

Task: Determine the programming for individual telephones and devices attached to BRI module S-loops.

- "Configuring an ISDN telephone DN record" on page 204
- "ISDN overview" on page 535

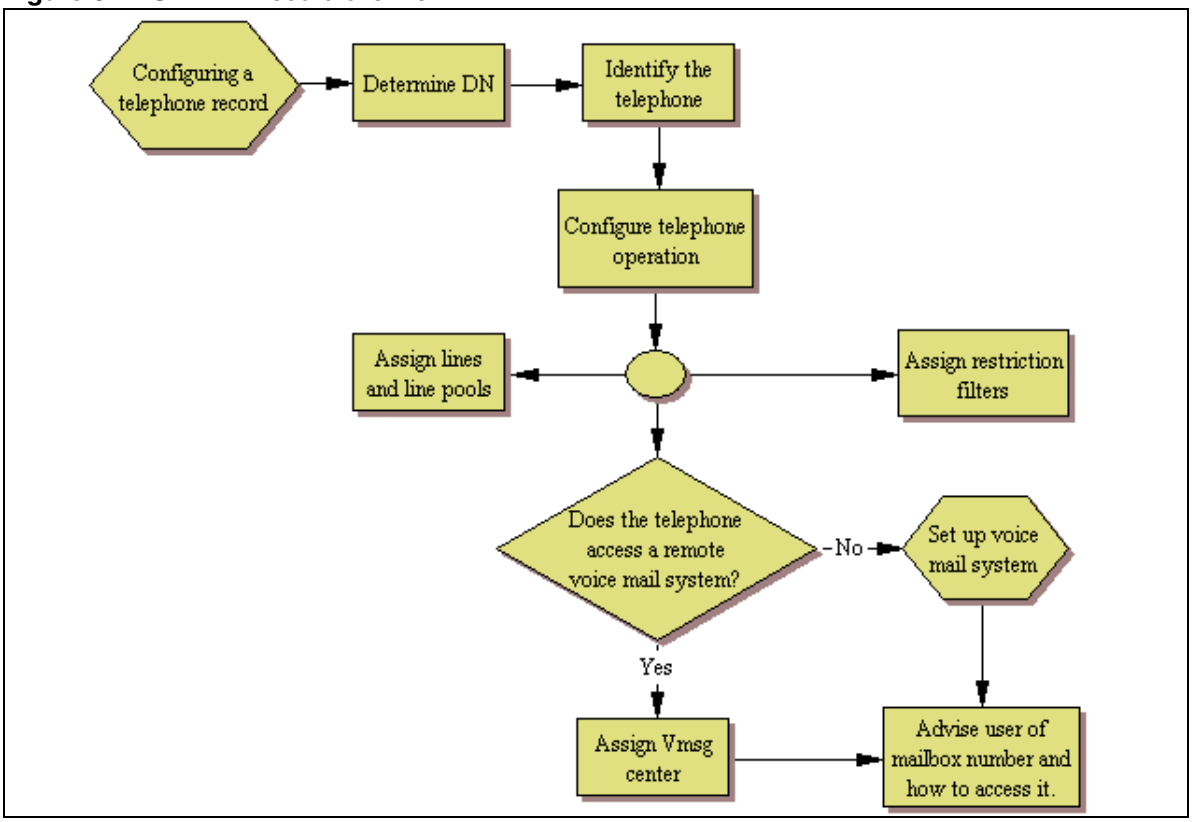
For a detailed description of DN record panels, and DN record procedures, see "DN records parameters" in the *Device Configuration Guide* (NN40020-300).

ISDN devices have a DN range that is unique to ISDN devices.

Process map

Figure 64 provides an overview of the ISDN DN record configuration process.

Figure 64 ISDN DN record overview


Configuring a telephone record
Determine DN
Identify the telephone
Configure telephone operation
Assign lines and line pools
Assign restriction filters
Does the telephone access a remote voice mail system?
No
Set up voice mail system
Yes
Assign Vmsg center
Advise user of mailbox number and how to access it.

Prerequisites

Ensure that the following prerequisites checklist is complete before configuring the devices.

BRI module installation and configuration is complete. Refer to "Trunk Module Parameters" on page 104.	
BRI loops programming is complete. Refer to "Setting BRI properties for ISDN device connections" on page 201.	
Lines are provisioned and configured. Refer to "Provisioning module lines/loops" on page 112.	
Wiring and network connections for the devices are complete.	

Configuring an ISDN telephone DN record

On each panel on the DNs list, add or modify settings to customize the telephone operations. The following headings correspond to each panel. Refer to the **Programming notes** in each section for configurations that are unique or specific for ISDN telephones.

Table 36 ISDN device-specific DN record settings

Affected field	Setting	Panel name and link to common procedures
Name	Unique to each device or device loop	"System DNs - Line Access tab" in the *Device Configuration Guide* (NN40020-300)
Call forward	Not supported	
Line appearances	Ring only	"Line Assignment and Line Pools" in the *Device Configuration Guide* (NN40020-300)
Answer DNs	Ring only	
Intercom keys	two: not configurable	"Configuring Capabilities and Preferences" in the *Device Configuration Guide* (NN40020-300)
The following settings are the only capability settings that require specific configuration for ISDN devices.		
Page settings	Page only- select. Devices cannot be assigned to Page zones.	"Configuring telephone capabilities" in the *Device Configuration Guide* (NN40020-300)
OLI as called number	<check box>	If Enabled, the specified OLI for the telephone is used for CLID for calls.
All other settings are variable, based on your system requirements.		

Chapter 22
Configuring CLID on your system

The following describes the various areas in the system that need configuration to allow incoming or outgoing Calling Line Identification Display (CLID) information to display (incoming calls) or transmit over the trunks (outgoing calls).

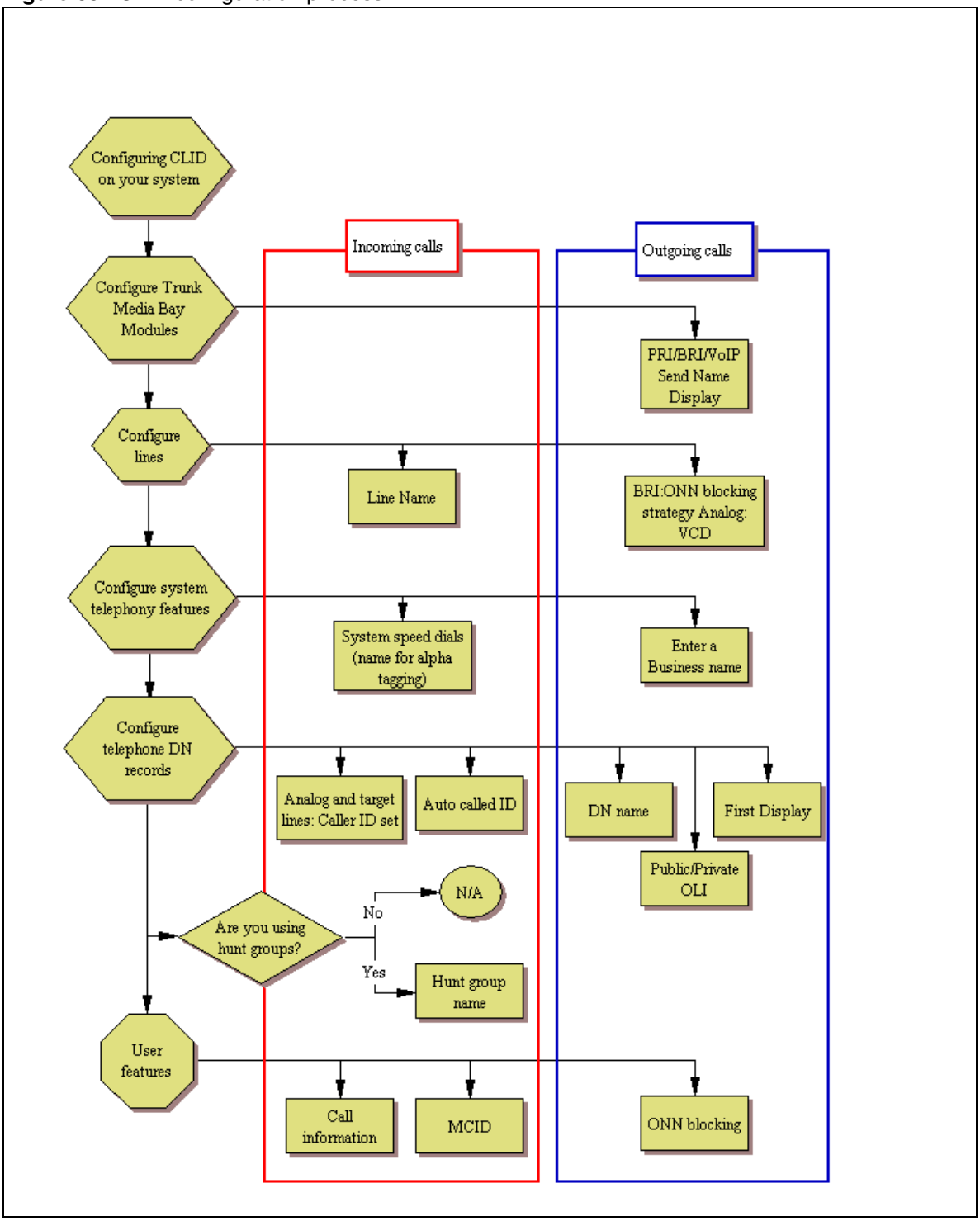
The following describes programming and setting up this feature.

Tasks:
Set up incoming display: “Programming incoming CLID” on page 207
Set up outgoing display: “Programming outgoing CLID” on page 208
Set up the method for blocking outgoing set identification: “ONN Blocking (North American systems)” in the *Device Configuration Guide* (NN40020-300)

Process map

Figure 65 provides a quick view of the areas of the system that need programming to provide incoming and outgoing CLID services.

Figure 65 CLID configuration process



Programming incoming CLID

Telephones can receive Name, Number, and Line display for incoming calls over trunks that support CLID or between telephones within the system. The following describes the different areas where these capabilities are configured.

Note: If no configuration is done, CLID will show up after answering a call unless Feature 811 is used. To make CLID appear before answer, you must set the Caller ID set on the set programming.

Digital, analog, and VoIP lines support CLID for incoming calls, and no special programming is required for the feature on these lines for BCM digital or IP phones.

Allowing CLID for telephones (incoming)

Target lines and analog CLID trunks connected to a GATM:

1. Click **Configuration > Telephony > Sets > Active Sets > Line Access**, and then select the DN record for a telephone assigned with analog lines that support CLID.
2. On the **Line Assignment** tab, select a line that supports CLID.
3. Select the check box beside the **Caller ID Set** field of the highlighted row.
4. Repeat for each line assigned to the telephone.
5. Repeat above steps for telephones assigned with these lines.

Note: Only 30 telephones can be assigned CLID for a line.

Using alpha tagging for name display (incoming)

To set up alpha tagging on your system

1. To determine the name to display, you add a system speed dial for the number, entering a display name. Refer to “Configuring system speed dial numbers” in the *Device Configuration Guide* (NN40020-300).

Note: You can increase the default number of system speed dials from 70 to 255 if you want to provide an extensive CLID list.

2. To determine how many digits of the dialed number and the system speed dial must match before a name is displayed, you set the **Clid match length** setting to the required number (1 to 8).

3 In order for the telephone to display the name, it must have **Caller ID** set for the line assigned to the telephone. Refer to "Line Access - Line Assignment tab" in the *Device Configuration Guide* (NN40020-300).

4 Set **First display** to **Name.** Refer to "Capabilities and Preferences main tab" in the *Device Configuration Guide* (NN40020-300).

Programming line name display (incoming)

Answered calls can display the name, incoming number, and line name/number for calls coming in over lines that allow full CLID.

Lines are named by their number as a default. However, you can provide a more descriptive identifier. The Name field is located on the main table under **Configuration > Telephony > Lines** ("Trunk/Line Data, main panel" in the *Device Configuration Guide* (NN40020-300)).

On the Hunt group record (**Configuration > Telephony > Hunt Groups > Hunt Groups** table), you can change the Hunt group Name field from the Hunt group DN to a more logical label for the group. Note that only eight characters display. Refer to "Hunt Groups system setup" in the *Device Configuration Guide* (NN40020-300).

Programming outgoing CLID

Telephones can transmit a business name, telephone name and number (outgoing line identifier) for outgoing calls over trunks to switches that support outgoing name and number (ONN) display, or between telephones within the system. This following describes the different areas where these capabilities are configured.

Programming Business name display (outgoing)

Nortel recommends that you use a blank space for the last character of the Business name to act as a separator between the Business name and telephone name.

Note that if you leave this field blank, no name appears.

To program the Business Name, select **Configuration > Telephony > Global Settings > Feature Settings**.

To program the Business Name

1 Click the field beside Business Name.

2 Type a maximum of eight characters for a name.

Leave a blank space for the last character of the Business name to act as a separator between the Business name and telephone name.

3 Other areas that you must program include:

- The **OLI number**. Refer to “Line Access tab” in the *Device Configuration Guide* (NN40020-300).
- The **Auto Called ID** must be selected. Refer to “Capabilities tab” in the *Device Configuration Guide* (NN40020-300).

Internal name and extension display

If you want to be able to see the CLID of internal telephones you call, ensure that Auto caller ID is enabled under **Configuration > Telephony > Sets > All DNs > Capabilities and Preferences**. Refer to “Capabilities and Preferences main tab” in the *Device Configuration Guide* (NN40020-300).

Programming name display (outgoing)

You can program name display for individual telephones.

On the DN record, you can change the Name field from the DN to a more logical label (**Configuration > Telephony > Sets > All DNs**). Note that only eight characters display. Refer to “Main panel tabs: common fields” in the *Device Configuration Guide* (NN40020-300).

Programming outgoing number display (OLI)

You can determine what number displays at the other end of an outgoing call, if the outgoing line allows name display and the receiving telephone has number display active.

Note: OLI is not supported on analog trunks.

The Outgoing Line Identification (OLI) can be set for each telephone for both private and public network calls.

The Private OLI is used for CLID over private networks. It is usually set to the DN number as a default, although this does not always occur if DN length changes have occurred. (**Configuration > Telephony > Sets > All DNs > Line Access** table). Refer to “Line Access tab” in the *Device Configuration Guide* (NN40020-300). If the system is running with a UDP dialing plan, you might want to add the LOC to the DN. Refer to “Outgoing private calls routing” on page 287.

The Public OLI is used for CLID over public networks and for tandem calls over private networks that terminate on the public network. The number of digits for this field is determined by your local service provider. (**Configuration > Telephony > Sets > All DNs > Line Access** table). Refer to “Line Access tab” in the *Device Configuration Guide* (NN40020-300).

Blocking outgoing name display at the trunks

To block outgoing name display at the media bay module level, you can configure module records to disable the Send Name display check box, select **Configuration > Resources > Telephony Resources > Trunk Module Parameters** (not available for all trunk types). Refer to "Trunk Module Parameters" on page 104"Trunk Module parameters" in the *Device Configuration Guide* (NN40020-300).

Blocking outgoing name display at the telephone

ONN is also enabled and disabled from a telephone, on a per-call basis, using **FEATURE 819**.

To allow **FEATURE 819** to work correctly, you may need to specify an ONN blocking service code.

The BCM alerts the CO by two methods. The method used depends on the type of trunk involved in placing the outgoing call. This information is supplied by your service provider.

- Analog trunks use a dialing digit sequence called a Vertical Service Code (VSC). The VSC differs from region to region and must be programmed. Analog trunks with both tone and pulse dialing trunks can have separate VSCs.
- PRI trunks have only one VSC. No specific system programming is required.

  ETSI note: ETSI lines may use the Calling Line Information Restriction (CLIR) supplementary service to provide this feature.
  ETSI PRI lines do not use a VSC. The line always uses Suppression bit to invoke the CLIR supplementary service.
- BRI trunks can be set to either:
  - provide ONN using a suppression bit, which provides a notice from the system to the central office to withhold CLI.
  - provide ONN using a VCS, which is dialed out in front of the dialed digits (optional on ETSI trunks).

  BRI trunk ONN settings are located under the loops settings. Refer to "BRI ISDN: BRI T-loops" on page 195"BRI ISDN: BRI T-loops" in the *Device Configuration Guide* (NN40020-300).

Programming note: Ensure that users who have access to this feature have telephones with valid OLI numbers.

Chapter 23
CLID: Name display

BCM displays the name of the calling party at the answering telephone when this information is available on Private or Public PRI trunks, VoIP trunks, and analog trunks that support Calling Line Identification (CLID). The displayed name can include the Receiving Calling Name, Receiving Redirected Name, and/or Receiving Connected Name. Refer to "Receiving and sending calling party name" on page 212.

If only a number is available for CLI on an incoming call, you can program a system speed dial in such a way that a name displays when that number calls in. Refer to "Alpha tagging for name display" on page 212.

Name and number information are also transmitted with outgoing calls. This can be blocked by the user (**FEATURE 819**) on a per-call basis. As well, you can block this information on a per-trunk basis. This is important if the connecting system cannot process name and number information. Some service providers also may have different codes that need to be mapped so that the blocking feature works.

Table 37 provides a list of the name/number display features and the list of ISDN interfaces that support each feature.

Table 37 Call features/interface list

Feature	Interface					
	NI PRI	DMS Custom PRI	SL-1 (MCDN)	NI-BRI	ETSI Euro (PRI/BRI)	ETSI QSIG
Receiving Calling Name	Supported	Supported	Supported	Supported		Supported
Receiving Redirected Name	Supported		Supported	Supported		
Receiving Connected Name		Supported	Supported			Supported
Sending Calling Party Name	Supported	Supported	Supported			Supported
Sending Connected Name		Supported	Supported			Supported

Note: Name Display is an optional feature that is available based on the interface to which you subscribe.

Note: MCDN networks fully support name display features within the private network environment.

Receiving and sending calling party name

Network Name Display displays the name of an incoming PRI/BRI, analog with CLID, or VoIP with MCDN call on the BCM telephone receiving the call.

Calling Party Name with status of Private can appear on the Called Party telephone as Private name. If the incoming Calling Name is defined by the CO as a private name, then Private name appears on the answering telephone. If the Calling Party Name is unavailable it can appear on the Called Party telephone as Unknown name.

If the call is answered by a Hunt group, the hunt group name appears instead of the telephone name in forming the connected name.

The Connected Name is a transient display that appears for approximately three seconds. The Connected Name is sent only if the OLI is programmed. You can program both a public and private OLI. The system uses the one appropriate to the type of call.

Network name display interactions

Calling and Connected Name information (if available) passes between trunks with Selective Line Redirection (SLR). Only Calling Name information passes between trunks in cases where Direct System Inward Access (DISA) results in tandeming of trunks.

Outgoing name display

You can set up the trunks to disallow name display to be sent out on PRI, BRI, and VoIP trunks. Use this for trunks where the connecting switch does not support outgoing line display. Default is enabled.

Business name display

Nortel recommends that you use a blank space for the last character of the Business name to act as a separator between the Business name and telephone name. A maximum of eight characters is supported.

Alpha tagging for name display

You can configure your system to display a caller name for incoming calls that provide number-only CLID, such as if the name service is not subscribed to or available in your area.

Note: Lines that provide name and number CLID, such as PRI lines, use that name for display, rather than the alpha tagging feature.

Limitations:

- Due to system resource limitations, only 30 telephones can be assigned to provide alpha tagging CLID per line.
- If the incoming number only partially matches the CLID match length, no name displays.
- If the number matches more than one speed dial, and the matches have different names, the telephone displays the name of the first match.
- ISDN devices do not support the alpha tagging feature.

Name display

You can assign names to identify your company, external lines, target lines, and your colleagues' telephones. During a call, the name (if programmed) appears on the telephone display instead of on the external line number or internal telephone number of the caller.

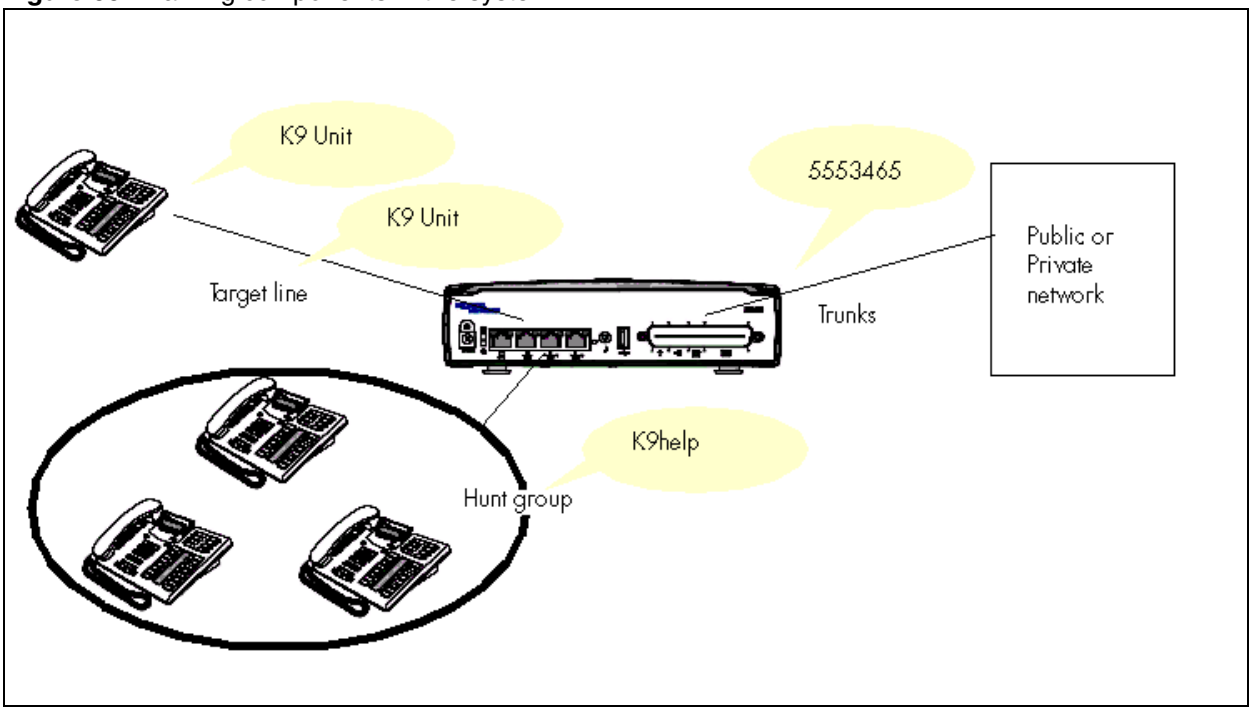
Names can contain both letters and numbers, but cannot be longer than seven characters. You cannot use the number (#) and star (*) symbols.

Note: You can give the same name to a telephone and a line in your system. Use initials, abbreviations, or even nicknames to give each telephone a unique name to avoid confusion.

You can also determine if the calling line ID (CLID) is received by a telephone, or if the CLID information from a system telephone gets sent out over the network. Refer to "Incoming and outgoing call display" on page 214.

Figure 66 illustrates an example of naming system components.

Figure 66 Naming components in the system



Incoming and outgoing call display

If you subscribe to Call Display services from your local telephone company, one line of information about an external caller appears on the display after you answer a call. If you answer before the Call Display information appears on your display, press **FEATURE 811** to view the line number or line name. When you transfer an external call to another telephone in your system, the same information appears on the recipient telephone display.

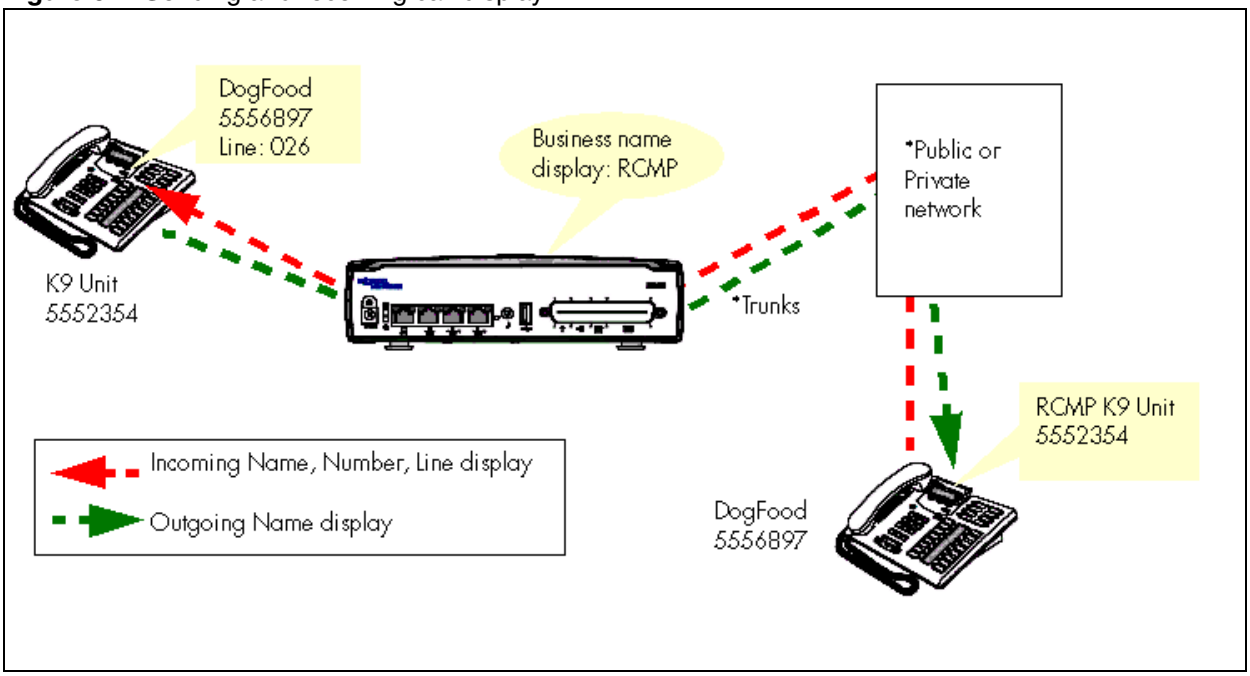
Depending on the services you subscribe to, incoming Call Display information can contain up to three parts:

- the name of the caller
- the number of the caller
- the name of the line in your system that the call is on

Call display information can also be sent out when a system telephone calls out of the system. What displays at the called party's telephone, depends on what the private or public lines allow. Outgoing call display information can be allowed or blocked at the system level or single telephone level.

Figure 67 illustrates an example of incoming and outgoing call display.

Figure 67 Sending and receiving call display



Chapter 24
Dialing plans

The BCM allows for flexible dialing plans using access codes, destination codes, PSTN trunks and private network trunks that provide multiple options for customizing the dialing options to meet each customers unique requirements. Refer to "Outgoing call routing" on page 222.

While the BCM can be plugged in and used immediately, it is recommended that you plan and execute the appropriate dialing plan.

The dialing plan includes:

- the dialing plans that govern the expected dialing strings on a private network
- the allowed dial strings on a public network
- the access and destination codes that get dialed out as part of the dialing string
- access codes that identify a call type on incoming MCDN calls

Refer to the following topics:

- "Creating dialing plans" on page 218
- "Public and Private Received numbers" on page 221
- "Private network dialing" on page 221
- "Setting up public network dialing" on page 221
- "Outgoing call routing" on page 222
- "Incoming call routing" on page 224
- "Determining line access dialing" on page 228
- "Understanding access codes" on page 229
- "Line pool access codes" on page 234
- "Using Carrier codes" on page 234
- "Configuring call routing" on page 234
- "Configuring Call-by-Call services" on page 235
- "Using destination codes" on page 239
- "Setting up VoIP trunks for fallback" on page 244

Also refer to "Call security: Restriction filters" on page 433. This section also discusses Class of Service (CoS) passwords, which you can use so that users can access the system features over public connections. Refer to "Call security and remote access" on page 415.

Creating dialing plans

Dialing plans allow users to access the public network, to make calls, and to answer dial strings.

Access to and from and within your system is based on dialing strings and how the system adds or deletes digits from this sequence to route the call.

A dialing string is the numbers that the caller physically enters on a telephone or programs onto a memory key. This can also include numbers the system adds to a dial string when a call goes through call routing.

This process also includes how the receiving system reads the sequence. All of which means that coordination is required at both ends of the call to ensure that calls are routed correctly. This is especially important if calls need to be routed through your system, or through a remote system, to reach another node on the network.

Basic numbering: The first numbering that you set is your DN length (Start DN length) and Start DN and Public and Private Received # length. DN length and Start DN information is entered when the system is initially set up. These numbers can be changed after the system has been set up, but only at the risk of compromising other numbering in the system. If your system is part of a network, these numbers must be coordinated with the other nodes in the network to ensure that the network dialing plans are consistent. The Public and Private Received Number lengths take their sequence from the initial DN length, but this can be changed to accommodate local dialing requirements, the Private length should mirror the DN length, except in special circumstances. Refer to "Incoming call routing" on page 224.

Variable	Example settings
Start DN	2 (221)
DN length, Received # length	
Private length	3
Public length (max)	12 (North America)

Remote access: When you set up lines that do not offer DISA directly on the line, you can determine if remote access prompts with DISA or allows auto answering. This determines the Public/Private Auto DN and Public/Private DISA DN settings, which are set under **Configuration > Telephony > Dialing Plan > Public Network and Private Network**. These numbers will have the same first number as you specified in the Start DN and be of the same length. Remote callers dial the system public or private access number, and then dial either the Private/Public Auto DN or Private/Public DISA DN, as determined by the line setup.

Variable	Example or default settings
Private Auto DN	2XX

Public Auto DN	2XX
Private DISA DN	2XX
Public DISA DN	2XX

Incoming calls: The Private Dialing Plan provides the special codes that identify the system to calls coming over private PSTN or VoIP trunks. Calls that do not match the private dialing plan information, are not accepted by the system.

Variable	Example or default settings
Private network ID	Number that identifies the system as part of the private network
Location code	UDP networks
Private DN length	DPNSS systems only

Calls coming in over private networks or PRI/BRI termination target lines can be set up for each telephone or group of telephones to which the calls are directed. As with other incoming calls, these calls can have a public or private call type that matches to a public or private received number assigned to a target line.

Variable	Example or default settings
Private received number	<CDP: same as DN of telephone> <UDP: LOC code + DN>
Public received number	<North America: 10 digits XXX-XXX-XXXX, the trailing digits are the DN> <DPNSS: maximum number of digits in local dialing pattern>

Outgoing calls: Other network codes include the information about public dialing codes that you enter under **Configuration > Telephony > Dialing Plan > Public Networks.**

The public dialing plan defines which dialing string prefixes will be allowed over the public PSTN lines. By defining these dial strings and the length of the prefix, the central office can direct the calls to the correct public destination.

Variable	Example or default settings
Public DN lengths (prefixes)	Public dialing table

For private networks, if you are not using routing and destination codes, you need to identify an access code that indicates an incoming call is destined for the private network.

Variable	Example or default settings
Private Access Code	6

MCDN special call types: If your system is networked to other types of systems, such as Meridian 1, which sends calls through one or more BCM systems to the public network, you need to specify specific call-type codes. These codes append to the incoming dial string, so that the call-type remains intact as it passes through the BCM call processing:

Variable	Example or default settings	
Local Access Code	9	Coordinate these settings with Meridian routing for these calls types and the Private Access Code.
National Access Code	61	
Special Access Code	911	

Internal feature access: Meanwhile, you need to keep in mind that the leading digit of any of the above dialing codes cannot conflict with the other system access codes that you want to use:

Variable	Example or default settings
Park Prefix	1 (101-125)
Direct Dial Digit	0

Line pool and destination access codes: Once these basic numbers have been picked, you can decide what numbers to use for line pool access codes and/or destination codes. The system will not allow these codes to start with any of the numbers currently assigned. If you are working with an established dialing plan, you may want to ensure that the numbers that the users are familiar with dialing are reserved for these codes.

For instance, if the users are familiar with dialing 9XXXXXXX to access numbers outside of their own offices, you will want to reserve this number for the destination codes. If you are setting up a new system, you could opt to use the location codes of the other systems as destination codes, or you could define one number for local calls (but which are still outside the system) and one number for long-distance calls. For example: The users may dial 6<DN number> for calls within a local system, but dial 8<area code><office code><extension or “DN”> for calls in another city over the public network.

Variable	Example or default settings
Line pool codes (first character)	5
Destination codes (first character)	6<up to 11 more characters> 9<up to 11 more characters>

Telephones use pool codes and destination codes to dial externally, because when the analog device goes off hook, it seizes internal dial tone from the system. The external access code, is either a line pool code, or destination code assigned to your system dialing plan.

Variable	Example or default settings
External code	9

Public and Private Received numbers

If the received number is different than the regular DN number, in the target line configuration programming, enter the number in the **Private number** and/or **Public number** field.

Programming note: Auto-answer trunks such as PRI, T1, BRI, and VoIP trunks, use these settings to route calls:

- DPNSS lines use the Private received number to route calls in the system.
- BRI (ETSI-QSIG), PRI (ETSI-QSIG, MCDN, DMS-100, DMS-250), and VoIP trunks route calls on a per-call basis to either the public or private received digits.

Note: VoIP trunking does not support Auto DN/DISA DN functionality.

- BRI (ETSI-Euro, NI), PRI (ETSI-Euro, NI, 4ESS), T1 (LoopStart, E&M, DID, GroundStart), Analog LEC (LoopStart), and DASS2 trunks route calls using the Public received number.

Private network dialing

If your BCM is part of a private network, you have a choice of dialing plans. However, all BCMs on a network must use the same type of dialing plan and have the same Private DN lengths to ensure proper call direction. Plan these settings before you start programming for the private network.

- UDP (Universal Dialing Plan) uses a destination code and a location code plus the set DN (that is, 6-403-XXXX) to determine where a call gets routed. You specify a Private DN length to allow all required digits to be dialed. Each node on the network has a unique location code.
- CDP (Coordinated Dialing Plan) uses a unique steering code that is transparent to the user and is dialed as part of the destination set's DN (that is, 2XXXX for one node, 3XXXX for another node, and so on) to determine where the call gets routed. Since each node on the network has a unique code, no other routing is required.
- The Meridian system administrator, or the call control system, generates the Private Network IDs. These IDs are unique to each node on a network. Both UDP and CDP must include this code in programming.

Setting up public network dialing

The public network settings allows you to enter DN lengths for the networks the callers are allowed to dial, including special numbers such as 411 and 911.

The public DN lengths table is used for all PRI calls except for those routes that use service type Private or service type TIE with DN Type specified as Private. This table allows the BCM to determine the length of a DN, based on the initial digits dialed.

A set of default Public DN lengths is included with the default template. In most cases it is not necessary to change the default values.

About the Public DN lengths table

In the public DN lengths table:

- You can define up to 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 to 25).
- Several entries are predefined in the North America profile. These defaults can handle most regions in North America without the need for additional programming. If required, you can remove or modify these entries.
- The table always contains one default entry. You cannot remove this entry. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

Outgoing call routing

Outgoing calls require line pool access codes or destination code (with defined routes) to leave the system.

- Access codes provide direct, unscheduled access to an analog, digital (T1).
- Destination codes also provide access to line pools, but they also allow more flexibility in dialing, which allows for more complex routing options, such as scheduling, fallback routing (VoIP trunks), call definition, and multiple routing (least-cost routing). Routing also allows you to minimize the dialout for the user, especially to systems on the same private network.

Outgoing calls can be either public or private, which is defined by the route. The public or private designation determines which dialing plan is used to determine the validity of the call. Normally, public calls are routed over PSTN trunks and private calls are routed over a private network. However, MCDN trunks can also pass calls designated as public to allow remote nodes on the network to call out of the PSTN of a local node. This is called tandem dialing.

- If the outgoing call is designated as private, the system checks the beginning of the string for a destination code that routes to a private network. It also checks that the dial string is the correct length. The destination code routing determines what the final dial string will be, adding or removing digits, as required.

- If the outgoing call is designated as public, the system checks the beginning of the string for a destination code that routes to a PSTN or an MCDN trunk. If the call routes to a public route, the system checks the public dialing table to ensure that the dialout string has legitimate leading digits and is the correct length. If the call routes to an MCDN trunk, the call is passed as dialed, minus the private networking codes. The call will pass through the system until the system with the matching destination code receives it, at which point it will be sent through the local PSTN of that system.

How the system identifies the call depends on the type of trunk chosen for the route. Refer to the table below.

Dialing plan setting	NPI/TON	Private called number length based on
MCDN trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/UDP	private access code + home location code (LOC) + private received digits
CDP	Private/CDP	private received digit
DMS-100/DMS-250/ETSI-QSIG trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/Subscriber	private access code + home location code (LOC) + private received digits
CDP	Private/Subscriber	private received digit

Outgoing public calls routing

Outgoing public calls from within the system typically have the routes set to Public. Refer to "Configuring call routing" on page 234. The NPI/TON gets sent as Unknown/Unknown. The public called number length is based on the Public DN lengths table in the Public networks dialing plan.

MCDN trunks also allow public call types when tandeming calls from another system on the private network. Some of these systems use specific call types that the BCM needs to recognize to pass on correctly. Also refer to "Using the MCDN access codes (tandem calls)" on page 232.

Type of call	NPI/TON	BCM prepend access code	BCM monitor display
Local	E164/Local	Local access code (9)	E.164/Subscriber
National	E164/National	National access code (X1)	E.164/National
Special calls (international, 911, etc.)	Private/Special	Special access code (9)	

Incoming call routing

Incoming call routing also depends on the call type. The system also uses the Public and Private DN length settings to determine call routing.

Defining DN length

The DN lengths setting allows you to change the number of digits for the Received number length and the DN length, which are used by the system to determine if an incoming call is valid for the system.

Each increase in length repeats the first digit in front of any existing DN. For example, if DN 234 was increased to a length of four, the new DN would be 2234.

Warning: Do not change DN length immediately after a system start-up. You must wait until the system is operational with two solid green status LEDs.

Warning: Increasing the DN length affects other areas of the system:

If the DN length change creates a conflict with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code changes to None, and the corresponding feature is disabled.

Optional applications affected by DN length changes:

Voice mail and **Contact Center** applications are reset if you change the DN length after these services are installed.

If you increase your DN length and then decide to decrease the DN length you will have to cold start your system and lose all of the programming.

Warning: If your system is running with a PBX telephony template, the Public and Private received # length are by default 3 (digits) at startup. Increasing the DN length after system startup does not change these digits, so you will need to manually change the Public and Private Receive Number length.

Private OLIs are automatically assigned to the DN records if the DN length and the Private Received Number length are the same. If this changes, the Private OLIs are cleared, or are not assigned (PBX template).

Network note: If your system is part of a private network, ensure that you confirm the dialing plan for the network before changing this length. If you change the length, ensure that you check all DN-related settings after the change.

Using the Received # length

If you change the DN length of your system, you may need to change the Received # length. Private and public networking, and the access codes to determine a route for an incoming call over an auto-answer trunk.

On systems running the DID telephony template, the Private and Public Received # length is set to the same length as the DN length for the system. On systems running the PBX telephony template, the Private and Public Received # length default to 3, unless the DN length is changed during the Startup procedure.

These digits identify target lines ("Processing incoming calls" on page 225), Auto DN*s*, and DISA DN*s*.

The received number can be shorter if network or central office constraints require this. This number cannot be greater than the system DN length on a networked system using a coordinated dialing plan (CDP) or a universal dialing plan (UDP). On a standalone system it is possible that the received number length would be greater than the DN length.

Warning: Decreasing the received number length clears all programmed received digits that are longer than the new settings.

Processing incoming calls

The system processes a call in the following way:

1. The system receives a call from the public or private network.
2. The system identifies the call type:

   Public calls:

   - If the call is from the MCDN network and is a local, national, or special call type, the system prepends the appropriate access code.

- If the call is from ETSI-QSIG, MCDN, NI, DMS-100, or DMS-250 and tagged as Private/Subscriber, the system prepends the Private access code, if the dialing plan is UDP.
- If the call is tagged as Unknown/Unknown or Private/Unknown (ETSI-QSIG, MCDN, N1, DMS-100, or DMS-250 trunks), no access code is added.
- For all other call types, the system truncates the trailing digits to the Public Received # Length. (Go to step 4)

Private calls:

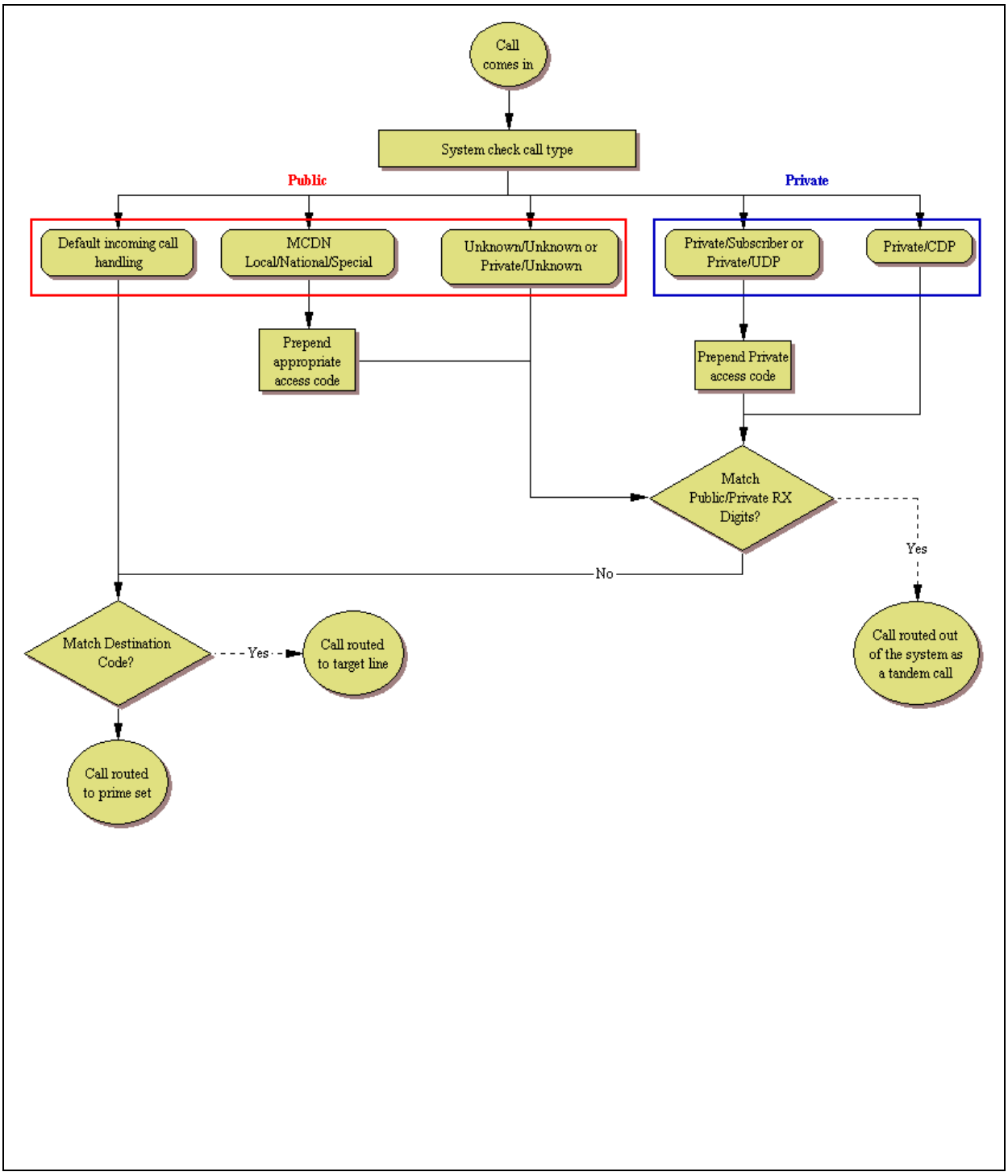
- If the call is tagged as Private/Subscriber or Private/UDP, the system prepends the Private access code.
- If the call is tagged as Private/CDP, no access code is added.

3 The system tries to match the first digits of the dial string to a destination code. If the digits match, the dial string is routed out of the system.

4 If the system cannot match the first digits to a destination code, the system tries to match the dial string to a target line (Public or Private Received Number). If the dial string does not match any target lines, the call is routed to the prime set for the line.

Figure 68 is a graphic illustration of incoming call processing.

Figure 68 Incoming public and private call coding



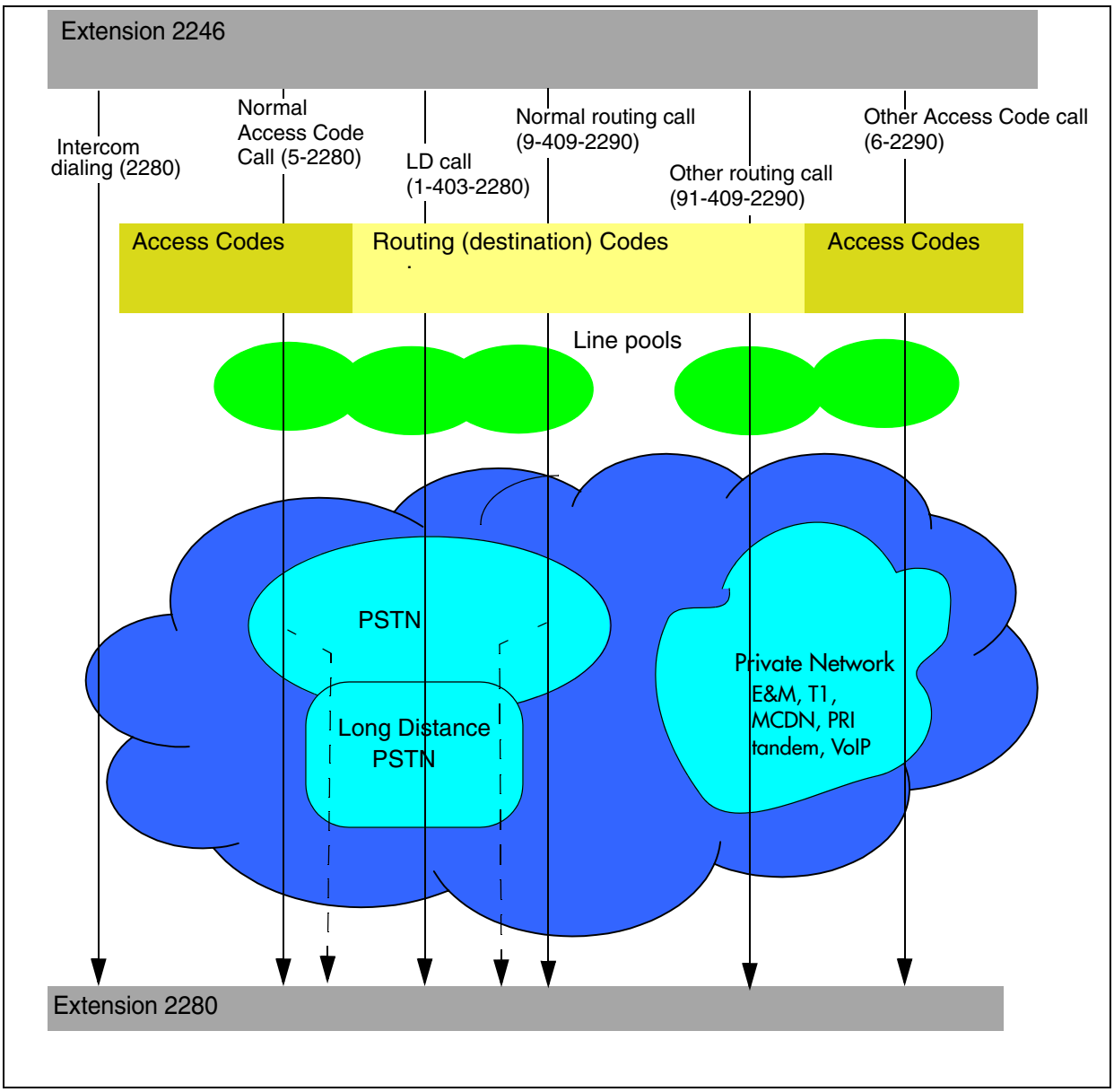
Determining line access dialing

"Understanding access codes" on page 229 and "Configuring call routing" on page 234 describe what you do with the lines and loops you previously set up into line pools.

By using access codes or call routing, which uses destination codes, you can determine which lines (routes) outgoing calls use. When you create a route, you can also specify restrictions that apply to how or when the line will be used.

Figure 69 provides an overview of how access codes and routing is used within the system to direct calls from a telephone in one system to a telephone in another system.

Figure 69 Line management diagram



Understanding access codes

The system uses access codes to direct calls to the correct lines and destinations. Refer to "Creating dialing plans" on page 218 for a general overview about using access codes within the system dialing plan.

Task:

Set up access codes for internal features:

- park prefix
- direct dial digit

Set up access codes that affect users dialing in from remote locations:

- Private Auto DN
- Public Auto DN
- Private DISA DN
- Public DISA DN

Set up access codes that affect calls coming in over the private network:

- Private access code
- Local access code
- National access code
- Special access code

Set up access codes that affect calls leaving the system:

- External code (ATA and analog devices)
- Line pool access codes
- Destination codes
- Carrier codes

The default settings shown in Table 38 can help you plan your access codes so there are no conflicts.

Table 38 Default codes table

Digit	Use	System panel
0	direct dial digit	Access codes
1	park prefix	Access codes
2XX	first digit of DNs/DN lengths	Set through Quick Start Wizard
9	line pool A destination code (Takes precedence over the External line destination code if there is a conflict.)	Routing

Call Park codes

When you park a call (**FEATURE 74**), the system assigns one of 25 codes for the retrieval of the call. You can then press the Page display key to announce the code that appears on the display.

These three-digit codes include the Call Park prefix, which can be any digit from 1 to 9, and a two-digit call number between 01 and 25. For example, if the Call Park prefix is 1, the first parked call is assigned Call Park retrieval code 101.

Note: The Park prefix must not conflict with the following:

- external code
- direct dial digit
- private access code
- Public/Private Auto DN
- Public Private DISA DN
- line pool code/destination code, or
- telephone DN

Note: Other programmable settings may affect which numbers appear in the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes.
If the DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

The system assigns Call Park codes to calls in sequence, from the lowest to the highest, until all the codes are used. The use of different of codes ensures a call reaches the right person, especially when more than one incoming call is parked.

Note: Model 7000 phones are supported in Europe only.

The highest call number (the Call Park prefix followed by 25) is used by model 7000 and 7100 telephones, analog telephones, or devices connected to the system using an ATA2. Analog telephones or devices cannot use the other Call Park codes.

When parking a code on an analog telephone, the call is parked on the highest park code. When retrieving a call, any phone can retrieve the call by entering the park code.

Calls are retrieved by pressing the intercom button and dialing the retrieval code. On model 7000 and analog telephones, pick up the receiver, if the call is parked by the analog phone, use the **<*parkcode*>25**; otherwise, use **<parkcode><parknumber>**.

Note: Analog phones can park call only at <parkcode>25.

You also need to program the park timeout. The park timeout determines when external parked calls that are not answered return to the originating telephone. See the *Device Configuration Guide* (NN40020-300) for information on programming park timeout.

You can disable Call Park by setting the Park prefix to None.

Creating Direct Dial sets

The Direct dial setting allows you to dial a single system-wide digit to call a specific telephone, called a direct dial telephone. The most common example of a direct dial set is a telephone for an operator, a receptionist or an attendant. You can program a maximum of five direct dial sets on the system, however, you can only specify one direct dial number for the system.

Tips about access codes

Here are some pointers to assist you in planning the access codes for your system.

Note: The following codes/digits must not conflict:

- park prefix
- external code
- direct dial digit
- private access code
- Public/Private Auto DN
- Public/Private DISA DN
- line pool code/destination code
- telephone DN

Note: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using "1" as an access code in a private network, conflicts with the PSTN numbering plan for long-distance calls.

- **External line access code**: If the DN length is changed, and the changed DNs conflict with the external line access code, the setting changes to None.
- **Direct dial telephone:** Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming.

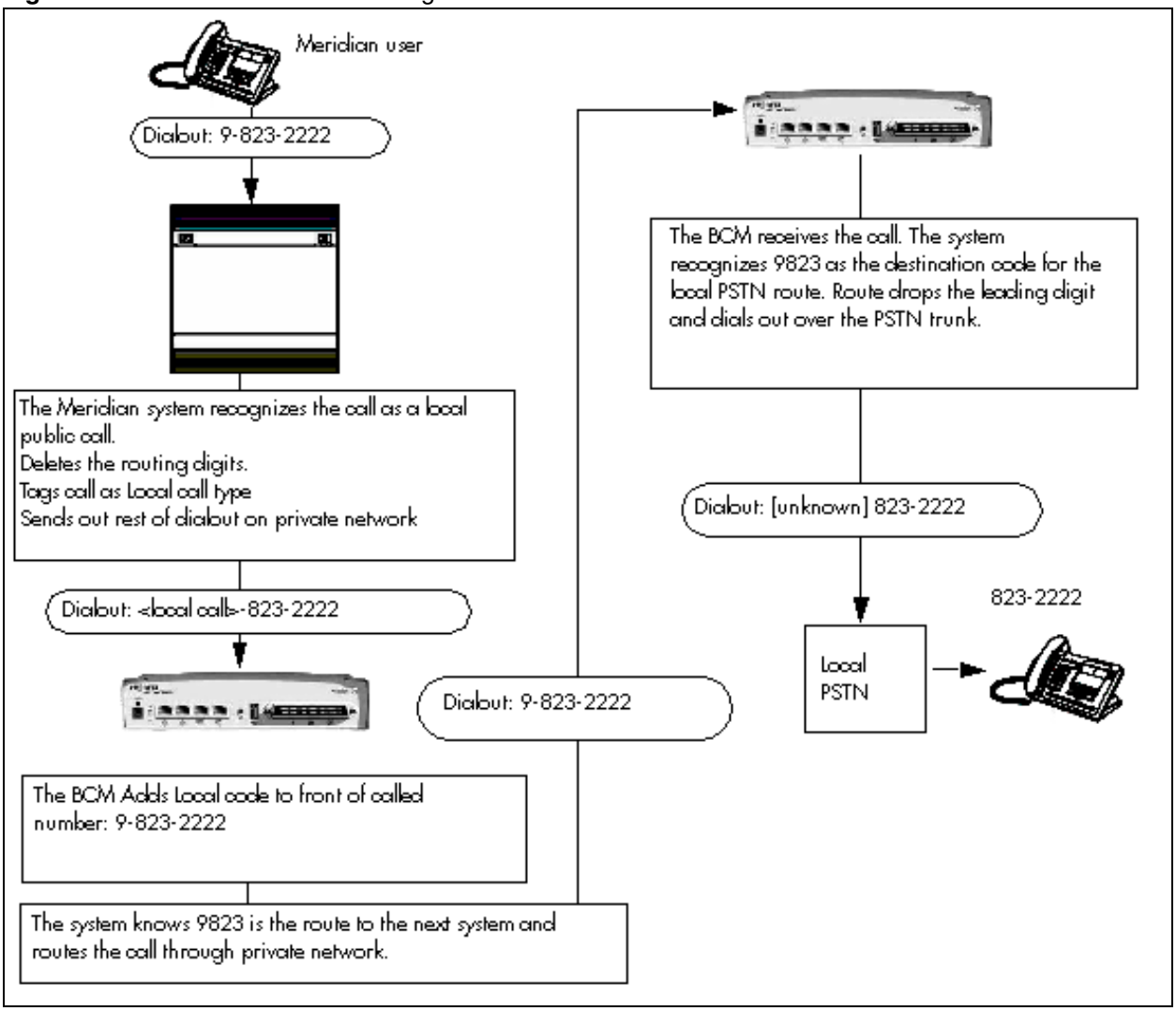
  If the DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.
- **Public/Private Auto DN:** The length of the Auto DNs are the same as the Public or Private Received Number Lengths specified under **Configuration > Telephony > Dialing Plan**. The public/private Auto DN is cleared if the corresponding Received Number Length is changed.
- **Public/Private DISA DN:** The length of the DISA DNs are the same as the Public or Private Received number length specified under **Configuration > Telephony > Dialing Plan**. The public/private DISA DN is cleared if the corresponding Received number length is changed.

Using the MCDN access codes (tandem calls)

Three special codes exist specifically for programming over PRI and VoIP trunks that are using the MCDN protocol, and which connect to a call server systems that use specific call codes for special call types, such as the Meridian 1 (M1). The purpose of the codes is to allow easier programming of the call server systems when calls are tandemed through a BCM to the local PSTN.

Calls tandeming to the public network through the private network need to retain their dialing protocol throughout the private network. This means that the BCM node receives a call from an M1 node tagged as a local call and recognizes the call intended for the public network, but also recognizes the call that needs to maintain the local call tag until it gets to the BCM node that is directly connected to the PSTN. This is accomplished by ensuring that the destination code, which starts with this access code, passes the call on using the route designated with the correct call type. Figure 70 charts this process.

Figure 70 Local call tandemed through BCM nodes


Meridian user
Dialout: 9-823-2222
The Meridian system recognizes the call as a local public call.
Deletes the routing digits.
Tags call as Local call type
Sends out rest of dialout on private network
Dialout: <local call>-823-2222
The BCM Adds Local code to front of called number: 9-823-2222
The system knows 9823 is the route to the next system and routes the call through private network.
Dialout: 9-823-2222
The BCM receives the call. The system recognizes 9823 as the destination code for the local PSTN route. Route drops the leading digit and dials out over the PSTN trunk.
Dialout: [unknown] 823-2222
Local PSTN
823-2222

Calls coming in from the public network need to be translated to their private network destination before routing/tandeming through the private network. In this case, the route used is defined with the call type of Private.

Line pool access codes

Line pool access codes allow you to assign an access code for each of the basic line pools (A to O). These codes specify the line pool for making an outgoing external call. Up to three digits in length, these codes do not allow any other routing programming. The user simply dials the code in front of the dial string. The system, in turn, deletes the entire code before sending the call out over the appropriate route.

If you need a more complex routing arrangement, you need to specify routes and destination codes, which allows you more flexibility in terms of dial strings, routing schedules, and routing restrictions.

Using Carrier codes

A multi-digit Carrier access code contains an Equal Access Identifier Code (CAC) followed by a Carrier Identification Code (CIC). The CIC identifies the carrier that handles the call. The Carrier Access Code table stores the CAC digit pattern that you define for your region.

In most cases it is not necessary to change the default values.

About Carrier access codes

Here are some general points about carrier access codes:

- You can define up to five carrier codes.
- Two entries will be predefined in North America, but you can remove these defaults.
- Each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 to 9).
- Each entry is identified by the prefix digits themselves.

Configuring call routing

Call routing allows you to define how calls are routed by your BCM system.

Call routing decides what path an outgoing call takes using the digits that are dialed. It is sometimes called Automatic Route Selection (ARS).

When you select an internal line and dial, the system checks the numbers you enter against the routing tables. If the number you dial starts with a destination code, the system uses the line pool and dials out digits specified by the route assigned to that destination code, and then dials the rest of the number that you dialed.

Routing service replaces a number of manual tasks, including:

- entering a line pool code

- dialing an access code for a long-distance carrier
- deciding which line pool to use according to the time and day

You can set up routing to take advantage of any leased or discounted routes using information supplied by the customer. The system cannot tell what lines are cheaper to use.

For Call-by-Call service selection (PRI only), the installer defines destination codes for various call types over PRI lines (for example, Foreign Exchange, TIE Trunk, or OUTWATS). The user dials a number using the intercom button without entering any special information. For more information see "Provisioning for Call-by-Call limits with PRI" on page 238.

Warning: Plan your routing service before you do any programming. Routing affects every call placed in the system and must be carefully planned to avoid conflicts and gaps in the programming. Use tables to design routes and destination codes, then check for potential problems before you start programming. It also saves you time when all the settings are written out in front of you.

Routing configuration

The settings for a call routing include:

- a three-digit route number (000-999)
- external # digits (up to 24 digits)
- a line pool
- destination codes (max. of 500 available, up to 12 digits)
- DN type and/or Service Type
- public and private DN lengths
- a schedule (optional)

Configuring Call-by-Call services

Call-by-Call service selection (CbC) allows you to access services or private facilities over a PRI line without the need for dedicated facilities. The different services represent different types of access to the network.

Refer to the following information:

- "Call-by-Call services" on page 236
- "Switches supporting Call-by-call limits" on page 237
- "Provisioning for Call-by-Call limits with PRI" on page 238

Supporting protocols

The following protocols support Call-by-call limits:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250
- AT&T 4ESS custom

Call-by-Call services

BCM supports the Call-by-Call Services listed in Table 39.

Table 39 Call-by-Call Services available on the system

Service	Description
Public	Public calls connect BCM and a Central Office (CO). BCM supports both incoming and outgoing calls over the public network. Dialed digits conform to the standard North American dialing plan (E.164 standard).
Foreign Exchange (FX)	Foreign exchange service connects a BCM site to a remote central office (CO). This provides the equivalent of local service at the remote location.
TIE	TIE lines are private incoming and outgoing lines that connect Private Branch Exchanges (PBXs) such as another BCM.
OUTWATS	Outward Wide Area Telecommunications: This outgoing call service allows a BCM user to call telephones in a specific geographical area referred to as a zone or band. Typically, a flat monthly fee is charged for this service.
INWATS	Inward Wide Area Telecommunications: This long-distance service allows a BCM user to receive calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
International INWATS	An international long-distance service that allows a BCM user to receive international calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
Switched Digital	This service provides premises-to-premises voice and data transport with call management and monitoring features.
Nine Hundred	This service is commonly referred to as fixed-charge dialing.
Private	Private incoming and outgoing calls connect BCM to a virtual private network. Dialed digits can conform to the standard North American dialing plan (E.164 standard) or the dialed digits can use a private dialing plan.

Switches supporting Call-by-call limits

Table 40 lists the service types and cross-references them with four common switches.

Table 40 Switches and service types chart

	Switches			
Service types[1]	**NI-2**	**DMS-100 (custom)**	**DMS-250**	**AT&T 4ESS**
FX	FX	FX[2]	N/A	N/A
Tie[3]	TIE	TIE	TIE	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International INWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTWATS	OUTWATS	PRISM	MEGACOM
Private		DMS Private[5]	VNET (virtual network)	N/A
Switched Digital	N/A	N/A	N/A	ACCUNET[4]
Nine Hundred	N/A	N/A	Nine Hundred	MultiQuest
Public	Public	Public	Public	N/A

1. N/A indicates that the protocol does not support the service.
2. DMS-250 Sprint and UCS support incoming FX only (that is, Network-to-BCM).
DMS-250 MCI does not support FX.
3. NI-2 allows two TIE operating modes: senderized and cut-through. BCM supports only senderized mode.
4. Rates greater than 64 kbps are not supported.
5. Bell Canada VNET.
6. Not all service types may be supported by a switch type. For information, contact your service provider.

Provisioning for Call-by-Call limits with PRI

To program the system for Call-by-Call Limits with a PRI interface, you must:

- provision a DTM as PRI, if one is not already configured as part of the system
- select a protocol
- program incoming call routing
- program routes that use the PRI pools, see "Configuring call routing" on page 234.

Other required programming in the Element Manager

Programming Call-by-Call on PRI requires these settings:

- Select **Configuration > Sets > All DNs** to assign the line pool.
- Select **Configuration > Telephony > Dialing Plan > Routing** to assign a pool for routing, and assign the service type and service id, if required.
- Select **Configuration > Telephony > Dialing Plan > Loops > Call-by-Call Limits** tab to specify the minimum and maximum values for the pools.

Call-by-Call service routing

Table 41 is an example of a Routing Table containing Call-by-Call programming (available in the North America market profile). Also refer to "Configuring Call-by-Call services" on page 235.

Table 41 Call-by-Call routing table example

Route Number (000-999)	Dial Out (24 digits)	Use Pool	Service Type	Service Identifier
003		BlocA	Public	
004		BlocA	FX	xxxxx
005		BlocA	TIE	xxxxx
006		BlocB	OUTWATS	xxx
007		BlocB	Private	
008		BlocB	Switched Digital	

Note: The public DN lengths are used for all PRI calls except those whose routes use service type Private or service type TIE with DN Type specified as Private.

Note: This type of routing applies only to those PRI trunks set with a protocol of NI, DMS-100, DMS-250 or 4ESS.

The service identifier (SID) depends on the selected service type (for example, with NI-2 protocol).

Service Type	Service Identifier description
Public	None
FX	Facility Number 1-5 digits
TIE	Facility Number 1-5 digits
OUTWATS[a]	Optional Band Number 1-3 digits
Private	None
Switched Digital	None

a. For NI-2, do not program the Carrier Access Code for banded OUTWAT calls. This call may be rejected.

When you select or change a PRI protocol, the Service Type and Service ID fields automatically clear for each entry in the routing table for that PRI.

PRI routing protocols

Table 42 lists the service/DN type choices available for PRI lines.

Table 42 PRI Service type/DN type values

PRI Protocol	Type	Values
MCDN	DN	Public, Private, Local, National, Special
ETSI Euro	DN	None, Overlap
ETSI QSIG	N/A	
NI	Service	Public, TIE, Foreign Exchange (FX), OUTWATS
DMS-100	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
DMS-250	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
4ESS	Service	TIE, OUTWATS, Switched Digital (SDS)

Using destination codes

Destination codes allow you to control how the system interprets and routes dial strings from internal sources. Destination codes are similar to line pool codes except that by using routes (which attach dial strings and DN type designators to line pools) and schedules you can control what digits the user has to dial and how the system routes the call out of the system, including what numbers from the dial string get added or deleted to the route dialout.

Note: Destination codes must not conflict with the following:

- park prefix
- external code
- direct dial digit
- Auto DN
- DISA DN
- Private access code
- line pool codes
- telephone DN
- public target line received digits
- other destination codes

Note: You can enter destination codes up to a maximum of 12 digits.

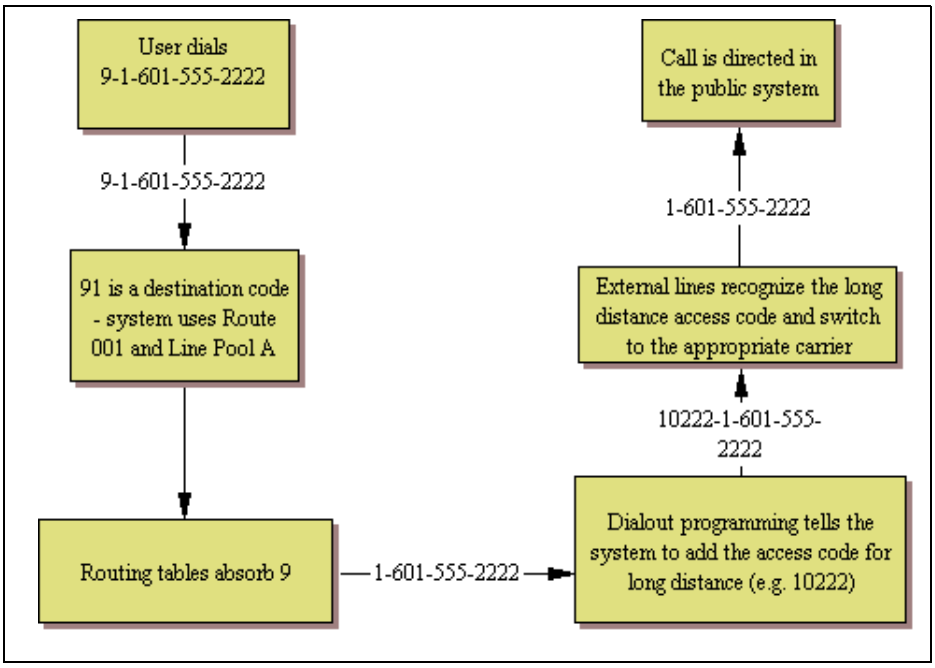
Why use destination codes?

Routes determine path (line or pool) and any required access numbers.

Destination codes determine which route to take (that is, an end node uses one destination code for all other nodes in the system). If you choose to use the destination codes Normal schedule, the call will always go out over the same route. If you choose to use the other destination codes schedules, you can set up a more responsive plan, whereby calls can go out over more than one route, based on scheduled times.

Destination codes provide you with the opportunity to create a dialing plan that allows users to connect to other systems in a relatively seamless or consistent manner, regardless of the lines or routes that are being used to get there. For example, connecting through VoIP lines requires significantly different ways of dialing than dialing over T1 lines. However, you can configure destination codes, such that the user dials the same number of digits regardless of the trunks over which the calls are routed.

Figure 71 Using destination codes to access another system


User dials 9-1-601-555-2222
9-1-601-555-2222
91 is a destination code - system uses Route 001 and Line Pool A
Routing tables absorb 9
1-601-555-2222
Dialout programming tells the system to add the access code for long distance (e.g. 10222)
10222-1-601-555-2222
External lines recognize the long distance access code and switch to the appropriate carrier
1-601-555-2222
Call is directed in the public system

Deciding on a code

Note: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using "1" as an access code in a private network, conflicts with the PSTN numbering plan for long-distance calls

When deciding on which digits to use to start your destination codes, consider the following:

- Ensure that the digit or digits you want to start your destination codes with do not match any of the access codes, including the line pool codes that already exist in your system.
  You may find that you need to delete line pool codes and create a route and destination code instead. This could occur if you want to set up fallback to a public line, for instance. If the public line is accessed by a line pool code, you would have to change access to a route so you could create a fallback schedule with the destination code used for the primary line (or lines, if you have more than one outgoing line pool that requires fallback).
- Decide how much of the common part of a dial string you want your users to have to dial, and how much you can put in the dial string.
- If you want specific dial strings to use specific routes, map these out first.

  For instance, if you want users to dial between BCMs over VoIP lines, you create destination codes specific to those systems that use the VoIP line pool, using the digits with which the users are familiar. You can then create a unique destination code for the call you want to route.

Example: If users are used to dialing 9-1-555-1234-<DN number> to reach another system (whose DN codes start with 6), you create a destination code of 915551236A, using the VoIP line pools (users dial the destination code plus the DN of the telephone they want to reach on the other system). The letter A at the end of the code represents any number from 0 to 9 which is not used by any other destination code.

If you need to use PSTN lines for a specific connection on the other system, you can create a destination code specific to that destination number and attach it to the route set up with the PSTN line pool (for example, 915551236333, 6333 being the DN of the device on the other system. When the user dials that specific number, the call will always go over the PSTN line). Note that by entering this code, users dialing with the code in the previous paragraph could never dial any DN that started with 63XX.

- If you want to use VoIP lines as your main lines, but you want to program one or more PSTN lines as fallback lines, you need to configure the routing and routing schedules so that the user dials the same number, regardless of which routes get used. You use the external number dialout string and absorb digits fields under the schedules in Destination code programming for this purpose.

- If a company wants to use VoIP lines between sites for interoffice calls, but not necessarily for all the voice traffic, they can configure specific destination codes for the VoIP routes. In this case, the destination code contains the same digits as a user would dial for a PSTN line, thus, making the shift transparent to the user and, at the same time, ensuring that the most economical route is being used. Depending on how many exceptions there are, you can use the wild card at the end of the string to save yourself from the necessity of entering a number of destination codes with the same leading digits.

Configuring Absorbed length

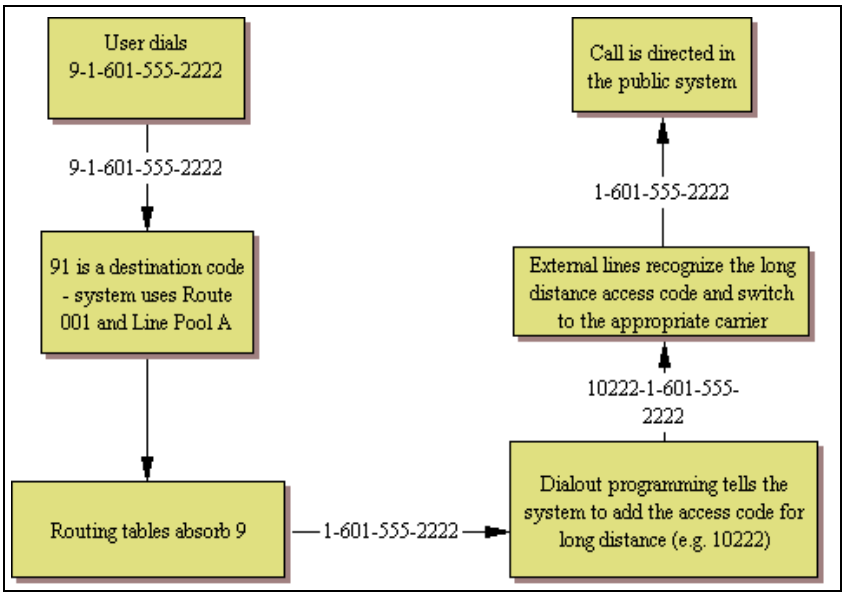
The digit absorption setting (**Absorbed Length**) applies only to the destination code digits.

When the Absorbed Length is at 0, the actual digits dialed by a caller are preserved in the dialout sequence. As you increase the absorbed length the equivalent number of digits are removed from the beginning of the destination code.

Adding Carrier access codes to destination codes

In some instances, long-distance service uses the same lines as local service but is switched to a specific carrier using an access number, which is sometimes referred to as a carrier access code (CAC). Route programming can include the access number so the users do not have to dial it every time they make a long-distance call. Figure 72 shows an example of how the system interprets what the user dials into a valid outgoing call.

Figure 72 Carrier code call numbering sequence


User dials 9-1-601-555-2222
9-1-601-555-2222
91 is a destination code - system uses Route 001 and Line Pool A
Routing tables absorb 9
1-601-555-2222
Dialout programming tells the system to add the access code for long distance (e.g. 10222)
10222-1-601-555-2222
External lines recognize the long distance access code and switch to the appropriate carrier
1-601-555-2222
Call is directed in the public system

Tips: The destination codes 9 and 91 used in the examples cannot be used together. If you need the destination code 91 to direct long-distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. You can also use 9 *A*. (*A* represents a wildcard "Any".)

Routing schedules and alternate routes

It can be less expensive to use another long-distance carrier at a different time of day. Continuing with the example used in the previous flowchart, the lines that supply local service in normal mode are also used for long-distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, you must build another route.

All the lines used by a route specified by a destination code are busy when a call is made, you can program other routes that the system automatically flows the calls to, or you can allow the call to overflow directly to the Normal route schedule (usually the most expensive route). However, this only takes effect if an active routing schedule is applied to the line. Overflow routing is not available in Normal mode.

You must create overflow routes for each destination code for which you want to allow overflow routing.

When a user dials, and the telephone cannot capture the preferred line (First Route), the system tries each successive defined route (Second Route, then Third Route). If none of these routes have available lines, the call reverts to the Normal mode. When the call switches from the preferred routing mode (First Route, Second Route, Third Route) to Normal mode, the telephone display flashes an “expensive route” warning. VoIP trunking uses a similar process for setting up fallback from the VoIP trunk to a PSTN line.

Note: Overflow routing directs calls using alternate line pools. A call can be affected by different line filters when it is handled by overflow routing.

Setting up VoIP trunks for fallback

Fallback is a feature that allows a call to progress when a VoIP trunk is unavailable or is not providing adequate quality of service (QoS).

Refer to “Setting up VoIP trunks for fallback” on page 391 for details about setting up fallback for VoIP trunks.

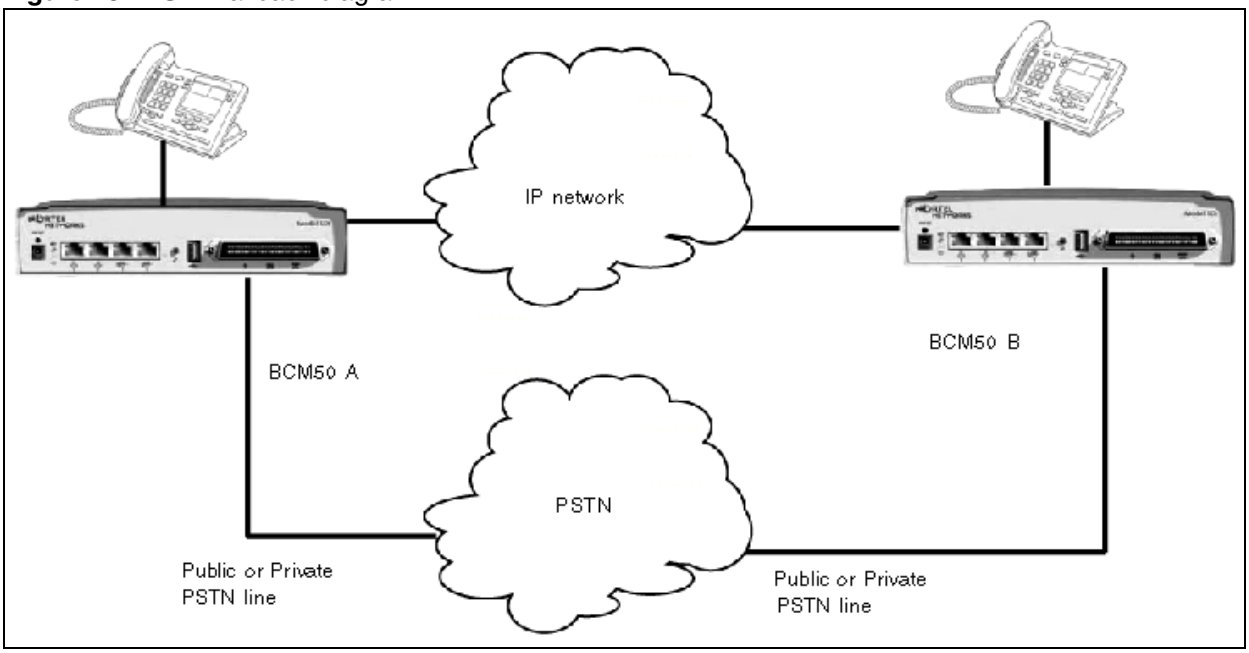
By enabling **Fallback to circuit-switched** on the **H323 Settings** panel, you allow the system to check the availability of suitable bandwidth for a VoIP call, then switch the call to a PSTN line if the VoIP trunk is not available or cannot produce the expected quality. The Local Gateway IP Interface panel is accessed at **Configuration > Resources > Telephony Resources > IP Trunks > H323 Settings**.

You use scheduling and destination codes to allow the call to switch from H.323 line pools to a PSTN line without requiring intervention by the user.

Use the dialing plan worksheet in the Programming Records to plan your dialing requirements so you can pinpoint any dialing issues before you start programming. If you are programming an existing system, you can look at what numbers the users are familiar with dialing, and you can attempt to accommodate this familiarity into your destination codes plan.

Figure 73 shows how a fallback network would be set up between two sites.

Figure 73 PSTN fallback diagram



In a network configured for PSTN fallback, there are two connections between a BCM and a remote system.

- One connection is a VoIP trunk connection through the IP network.
- The fallback line is a PSTN line, which can be the public lines or a dedicated T1, BRI, PRI or analog line, to the far-end system.

When a user dials the destination code, the system checks first to see if the connection between the two systems can support an appropriate level of QoS. If it can, the call proceeds as normal over the VoIP trunk. If the minimum acceptable level of QoS is not met, the call is routed over the second route, through the PSTN line.

For PSTN fallback to work, you must ensure that the digits the user dials will be the same regardless of whether the call is going over the VoIP trunk or the PSTN. In many cases, this involves configuring the system to add and/or absorb digits.

Chapter 25
Dialing plan: Routing configurations

This following describes how you can configure the lines and loops to allow system users to dial out of the system over a public or private network.

The following paths indicate where to access the route lines and loops in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Routing**
- Telset interface: ****CONFIG > Services > Routing Service > Routes**

Task: Set up routing for various call scenarios:

"Destination code numbering in a network" on page 249
"Setting up a destination for local calling" on page 249
"Setting up a route through a dedicated trunk" on page 250
"Grouping destination codes using a wild card" on page 251
"Programming for least-cost routing" on page 252
"Using multiple routes and overflow routing" on page 252
"Using the MCDN access codes to tandem calls" on page 257

Prerequisites

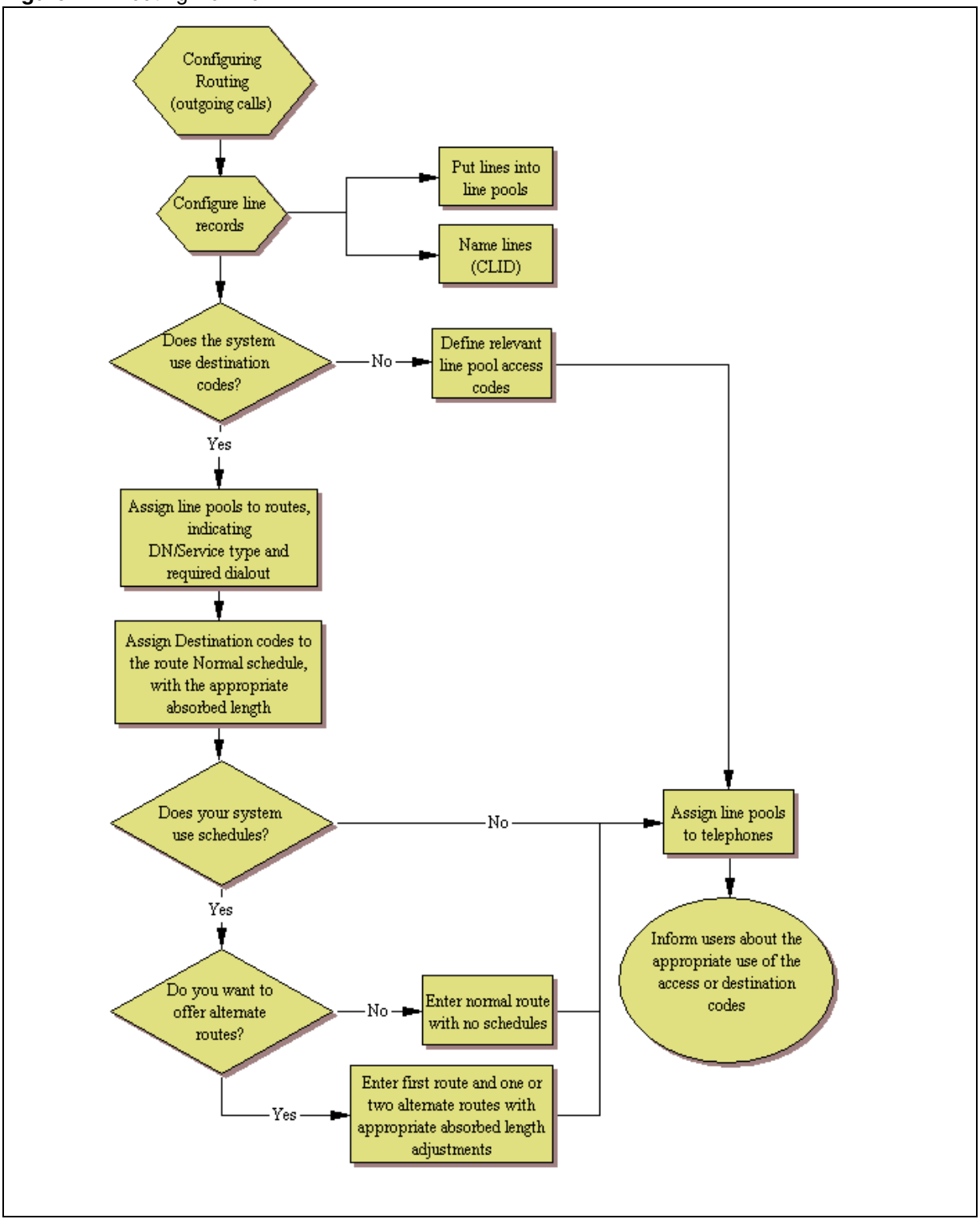
Complete the following prerequisites checklist before configuring the modules.

Media bay modules/VoIP trunks are installed and configured.	
Create an access code/route map to understand how the numbering works for the system.	

Routing work flow

Figure 74 shows an overview task flow for the areas in programming that affect how routes are set up.

Figure 74 Routing workflow


Configuring Routing (outgoing calls)
Configure line records
Put lines into line pools
Name lines (CLID)
Does the system use destination codes?
No
Define relevant line pool access codes
Yes
Assign line pools to routes, indicating DN/Service type and required dialout
Assign Destination codes to the route Normal schedule, with the appropriate absorbed length
Does your system use schedules?
No
Assign line pools to telephones
Yes
Inform users about the appropriate use of the access or destination codes
Do you want to offer alternate routes?
No
Enter normal route with no schedules
Yes
Enter first route and one or two alternate routes with appropriate absorbed length adjustments

Destination code numbering in a network

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits. Table 43 gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Table 43 Destination code leading digits

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
1	Call Park Prefix
9	All PSTN Calls
7	Unused

In Table 43, 4 is used as the initial digit for the coordinated dialing plan, but 5, or 6 can also be used for this purpose.

Tips: When programming a button to dial an external number automatically (autodial), private network calls must be programmed as external autodial numbers, even though they resemble internal extension numbers.
Routes generally define the path between the BCM system and another switch in the network, not other individual telephones on that switch.

Setting up a destination for local calling

An office can have different suppliers for local and long distance telephone service. By programming a destination code, any call that begins with 9, which is the most common dial-out digit, automatically uses lines dedicated to local service.

To build a route to allow local calls

1. Create a route that uses the line pool you assigned for the PSTN trunks. Refer to "Routes" on page 260.
2. Create a destination code record and enter a destination code, such as 9, which is a common local call code. Refer to "Grouping destination codes using a wild card" on page 251.

   For local calls only, there are no dial out numbers. Compare with "Setting up a route through a dedicated trunk" on page 250.

   The destination code can use a different route, depending on what schedule is assigned. In the current example, the route you define is used when someone dials 9 during Normal mode, when the other Schedules are turned off.

3 Set up the Normal schedule with the route number you defined in step 1.

Figure 75 Routing Service programming example

Routing Service (Services: Routing Service)		
Route # (000-999)	**Dial out (if required) (max. 24 digits or characters)**	**Use Pool**
001	none	A B C D E F G H I J K L M N O
002	none	A B C D E F G H I J K L M N O

Figure 76 shows an example of a destination codes programming record filled out.

Figure 76 Destination codes for call routing

Destination codes (Services; Routing service; Destination codes)								
Service Schedule (max. 7 char)	**Normal Rte**		**Route schedule**					
DestCode (max. 7 digits)	**Use route (000-999)**	**Absorb Length**	**1st route (000-999)**	**Absorb Length**	**2nd route (000-999)**	**Absorb Length**	**3rd route (000-999)**	**Absorb Length**
9	003	All						
1	002	0						

An office can have leased lines or private network trunks that provide cheaper to long distance calls by routing through the dedicated lines to remote systems, then using the local PSTN from that system to make the call. The routing should take place automatically when the number of the outgoing call begins with 1.

Setting up a route through a dedicated trunk

If your long distance is supplied by an alternate service or if you want to use different trunks at different times of the day, you can configure a route to use a specific trunk.

To set up a route through a dedicated trunk

1 Create a route that uses the line pool containing the discounted lines for long distance calling. Refer to "Routes" on page 260.

2 Create a destination code record and enter a valid destination code (maximum of 12 digits). Refer to "Grouping destination codes using a wild card" on page 251.

You must use a valid destination code, such as 91 (9, indicating PSTN; 1, indicating a long distance). View existing destination codes before entering a new code. The destination code can use a different route depending on the Schedule.

3 Under the **Normal** schedule for the destination code, enter the route you specified in step 1.

Grouping destination codes using a wild card

If you have a number of destinations that have the same route and digit absorb length, you can group these codes under one destination code to maximize your destination code table. In this case, the start digits will be the same, but the last character will be the wild card, and indicates any digit between 0 and 9. However, if a conflict exists with other digits already programmed or used by other destination codes, an error message appears.

For instance, you might use the same route (555) to a number of remote sites. Each site is accessed with the same external # (dial out string), except for the last digit, which is unique to each site. The exception to this is a site with a totally different access number and line pool requirement (route 565). This example is shown in Table 44.

Table 44 Establishing routes and dialout requirements

Route	Dial Out (external #)	Line Pool
555	0162 237 625<unique number from 0 to 9>	Line Pool C
565	0173 133 2211	Line Pool A

If you do not use wild cards, you would need to create a separate destination code for each unique dialout, as shown in Table 45.

Table 45 Destination codes not using a wild card

Destination codes	Route	Absorb Length	Dial Out
5621	555	3	0162 237 6251
5622	555	3	0162 237 6252
5623	555	3	0162 237 6253
5624	555	3	0162 237 6254
5625	555	3	0162 237 6255
5626	555	3	0162 237 6256
5627	565	All	0173 133 2211
5628	555	3	0162 237 6258
5629	555	3	0162 237 6259

If you use the wild card character *A (*ANY), you can reduce the number of destination codes you require to two, as shown in Table 46.

Table 46 Destination codes using the ANY character

Destination codes	Route	Absorb Length	Dial Out
562A	555	3	0162 237 625X where X is the last digit of the destination code dialed out, from 1 to 9, but not 7
5627	565	All	0173 133 2211

Tips: To minimize the effort involved in preparing destination codes, set the digit absorption to 0. When digital absorption is set to 0, the actual digits dialed by a caller are preserved in the dial-out sequence. The need to program a dial out sequence as part of the route depends on the required dialout.

Programming for least-cost routing

It can be less expensive to use another long distance carrier at a different time of day. Continuing with the example used in Figure 74, the lines that supply local service in normal mode are also used for long distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, you must build another route.

To build a route for a secondary carrier

1. Create a route for the trunks and assign it to the Normal schedule. Refer to "Setting up a route through a dedicated trunk" on page 250.
2. If all the required numbers are defined in the dial string, clear the **External Number** field.
3. Choose the line pool that contains the local service carrier lines.
4. Now you need to create a destination code and assign the route to the Night schedule. In this case, the change in route uses the start and stop times for Night Schedule.
5. Create 91 as a **Destination code**.
6. Make sure **Absorbed length** is set at 1.
7. Under **Night schedule:** enter the route you defined in step 1.

Calls that begin with the digits 91 travel out without using the access code when the Night schedule becomes active or when you turn it on at a control telephone.

Using multiple routes and overflow routing

If all the lines used by a route specified by a destination code are busy when a call is made, you can program other routes that the system automatically flows the calls to, or you can allow the call to overflow directly to the Normal route schedule (usually the most expensive route). However, this only takes effect if an active schedule is applied to the line. Overflow routing is not available in Normal mode.

You must create overflow routes for each destination code for which you want to allow overflow routing.

To set up the multiple routing overflow feature

1 You assign the preferred routes in a destination code schedule. Refer to "Alternate routes for routing schedules" on page 264.

   a Pick a schedule when you want these routes to be in effect.

   b In the **First Route** field enter the route number for the preferred route for the call.

   c Choose the absorb length for the first route that is appropriate for the dialout numbers you entered for the route.

   d Repeat steps b and c for **Second Route** and **Third Route** fields.

   e Define the start/stop time as 0100 under the equivalent Routing Services schedule. This setting means that the schedule is active 24 hours a day. Refer to "Configuring schedule names and timers" in the *Device Configuration Guide* (NN40020-300).

2 Assign an overflow route, usually the most expensive route, to the same Destination Code, but for the Normal schedule. Refer to "Destination codes" on page 262.

3 On the Scheduled Services table, choose auto for Service Setting, and enable Overflow. Refer to "Configuring scheduled service" in the *Device Configuration Guide* (NN40020-300).

4 Use a control telephone to activate or override the feature on the telephones on which you want preferred routing to be active.

Note: You must also ensure that the route correctly absorbs or passes dialed digits so that the number dialed for each line is the same from the user perspective.

When a user dials, and the telephone cannot access the preferred line (First Route), the system tries each successive defined route (Second Route, then Third Route). If none of these routes have available lines, the call reverts to the Normal mode. When the call switches from the preferred routing mode (First Route, Second Route, Third Route) to Normal mode, the telephone display flashes an "expensive route" warning.

Note: Overflow routing directs calls using alternate line pools. A call can be affected by different line filters when it is handled by overflow routing.

VoIP trunking uses a similar process for setting up fallback from the VoIP trunk to a PSTN line.

This following deals with applying the programming in network situations.

- "Dialing plan using public lines" on page 254
- "Destination code numbering in a network" on page 249

Dialing plan using public lines

Figure 77 and Figure 78 provide examples of how you can record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax, and Vancouver. Without routing, a BCM user in Toronto must to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number, the user simply dials 3027. The same feature is available for Vancouver (604).

In the column Dial-out, P stands for pause, a host system signaling option. Press **FEATURE 78** to insert a 1.5-second pause in the dialing string.

Figure 77 Routing service record: use pool

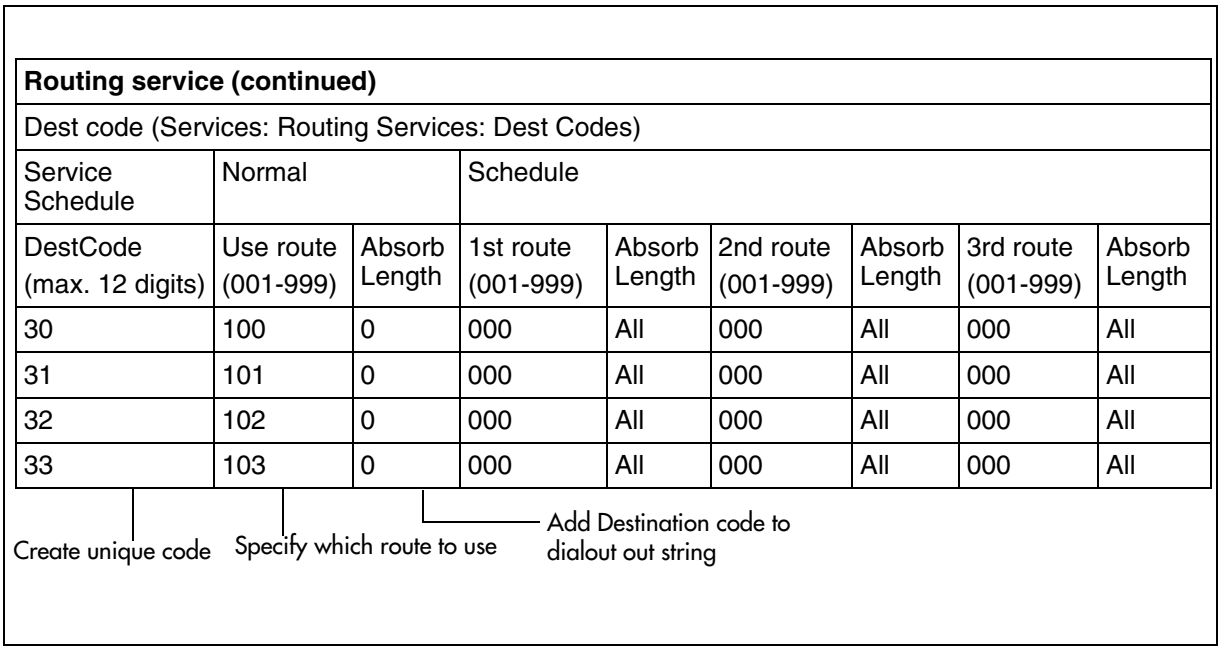
Routing Services (Services: Routing Service)		
Route # (000-999)	Dial-out (if required) (max. 24 digits or characters)	Use Pool
100	902-585	(A)BC
101	902-585	(A)BC
102	604-645	(A)BC
103	604-645	(A)BC

Create unique route number

Specify dial-out digits

Route through Pool A

Figure 78 Routing service record: Destination code



Routing service (continued)								
Dest code (Services: Routing Services: Dest Codes)								
Service Schedule	Normal		Schedule					
DestCode (max. 12 digits)	Use route (001-999)	Absorb Length	1st route (001-999)	Absorb Length	2nd route (001-999)	Absorb Length	3rd route (001-999)	Absorb Length
30	100	0	000	All	000	All	000	All
31	101	0	000	All	000	All	000	All
32	102	0	000	All	000	All	000	All
33	103	0	000	All	000	All	000	All

Programming the PRI routing table

The dialing plan must be thoroughly planned out in advance before you program the information into the BCM system.

To program the PRI routing table

1 Click **Configuration > Telephony > Dialing Plan > Routing**.

2 Click the route number record you want to use.

3 In the External Number column, type a dialout number (up to 24 digits).

4 Under Use Pool**,** select a PRI line pool.

The Bloc pools that are displayed depend on how you allocate PRI lines into pools in the line programming. It is possible to have only pool BlocA, or only pool BlocB, even if there are two DTMs configured as PRI in the system.

5 Choose a Service Type or DN type:

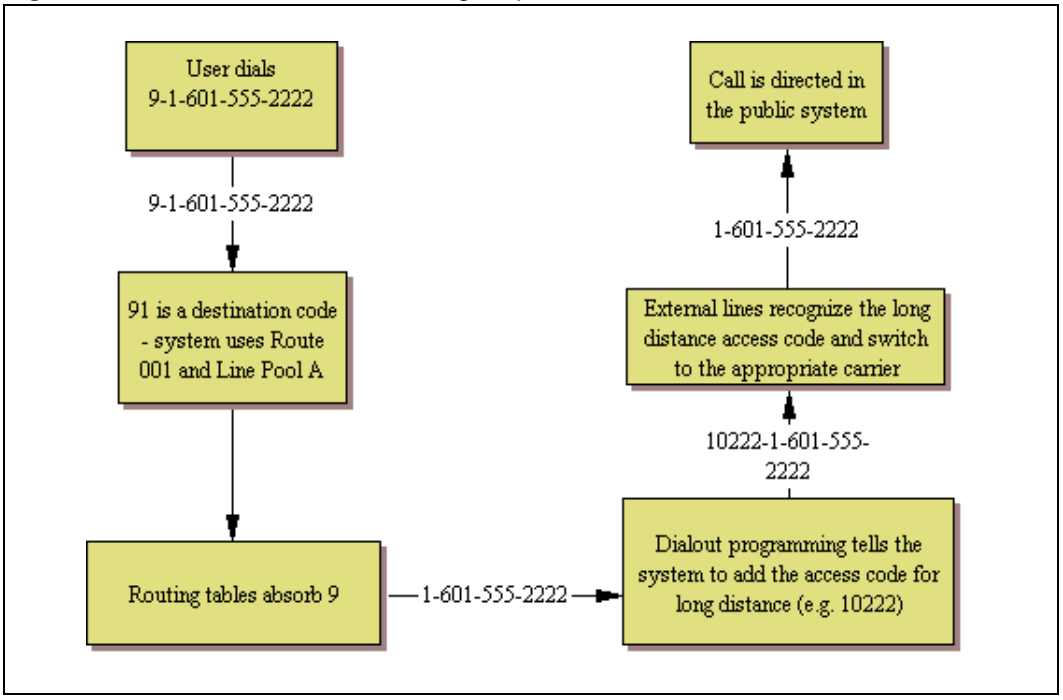
- **DN type:** displays for PRI lines with protocol set to SL-1 (MCDN, ETSI Euro).
- **Service type:** displays for PRI lines with protocol set to NI, DMS-100, DMS-250, 4ESS.
- **Service ID: N/A** appears where the service requires an ID.

Adding Carrier access codes to destination codes

In some cases, long distance service uses the same lines as local service but is switched to a specific carrier using an access number, which is sometimes referred to as an carrier access code (CAC). Route programming can include the access number so the users do not have to dial it every time they make a long distance call. Figure 79 shows an example of how the system interprets what the user dials into a valid outgoing call.

Note: Carrier code service must be supported from the Central Office.

Figure 79 Carrier code call numbering sequence


User dials 9-1-601-555-2222
9-1-601-555-2222
91 is a destination code - system uses Route 001 and Line Pool A
Routing tables absorb 9
1-601-555-2222
Dialout programming tells the system to add the access code for long distance (e.g. 10222)
10222-1-601-555-2222
External lines recognize the long distance access code and switch to the appropriate carrier
1-601-555-2222
Call is directed in the public system

To program a long distance carrier access code into a destination code

1. Create a route that uses a line pool containing local lines only. ("Routes" on page 260)
2. Program a route to use a line pool containing the lines used to access the long distance carriers.
3. Type the dialout digits, which are the same as the access digits. For example, if the access code is 10222, the dialout digits are10222.
4. Create a destination code 91: 9 (for outside access) and 1 (for long distance). You must use a valid destination code.

5 Set **Absorbed Length** to 1.
The digit 9 is only used internally and should be dropped. The 1 is needed to direct the call to the public carrier network.

Tips: The destination codes 9 and 91 used in the examples cannot be used together. If you need the destination code 91 to direct long distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. Refer to "Grouping destination codes using a wild card" on page 251 for information on programming destination codes.

Using the MCDN access codes to tandem calls

Three special access codes exist specifically for programming calls over PRI and VoIP trunks that are using the MCDN protocol, and which connect to a call servers that use specific call codes for special call types, such as the Meridian 1 (M1). The purpose of the codes is to allow easier programming of the call servers when calls are tandemed through a BCM system to the local PSTN. Refer to "Private Network Settings" on page 282 for a description of these fields in context with the private dialing plan.

This is how the codes relate:

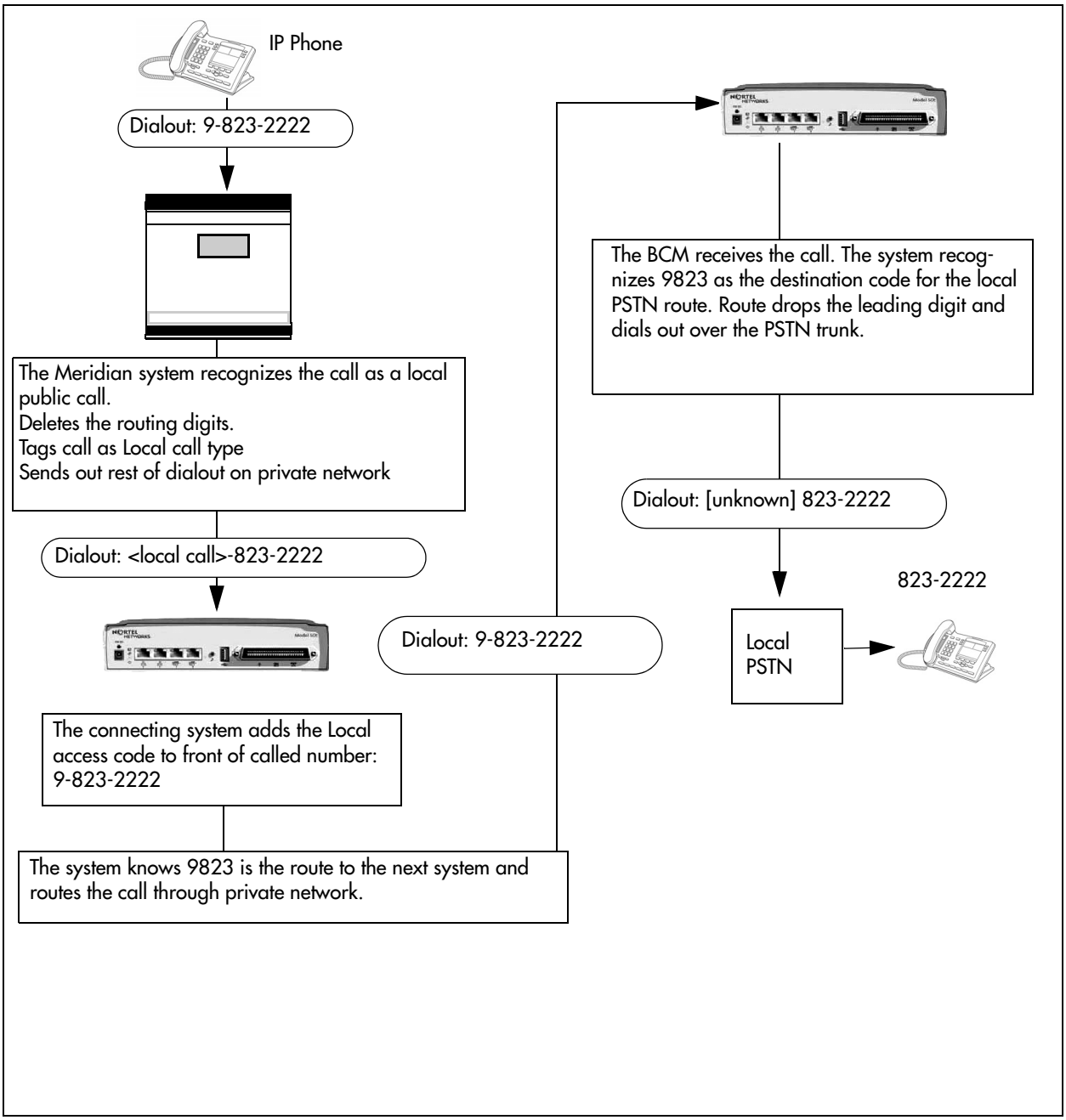
Meridian 1 access codes	BCM access codes	Sample code
Network/long distance code	Private access code	6
	National access code	61
Local code	Local access code	9
	Special access code	9

Calls tandeming to the public network through the private network need to retain their dialing protocol throughout network. This means that a call from an M1 node tagged as a local call gets received by the local node and is recognized as a call intended for the public network, but also as a call that needs to maintain the local tag until it gets to the local node that is directly connected to the PSTN. This is accomplished by ensuring that the destination code, which starts with this access code, passes the call on using the route designated with the correct DN type. Refer to "Setting up a route through a dedicated trunk" on page 250.

Calls coming in from the public network need to be translated to their private network destination before routing/tandeming through the private network. In this case, the route used is defined with the DN type of Private.

Figure 80 charts the process for a call tandeming through a BCM to the local public network.

Figure 80 Local call tandemed through private network nodes


IP Phone
Dialout: 9-823-2222
The Meridian system recognizes the call as a local public call.
Deletes the routing digits.
Tags call as Local call type
Sends out rest of dialout on private network
Dialout: <local call>-823-2222
The connecting system adds the Local access code to front of called number: 9-823-2222
The system knows 9823 is the route to the next system and routes the call through private network.
Dialout: 9-823-2222
The BCM receives the call. The system recognizes 9823 as the destination code for the local PSTN route. Route drops the leading digit and dials out over the PSTN trunk.
Dialout: [unknown] 823-2222
823-2222
Local PSTN

Chapter 26
Dialing plan: Routing and destination codes

A large system usually requires a number of destination codes to ensure that calls are directed to the correct trunks, either on the private or public network.

The following paths indicate where to access destination codes in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Routing**
- Telset interface: ****CONFIG > Services > Routing Service > Routes**

The following panels allow you to:

- create routes
- create destination codes for the routes, and the Normal schedule
- create alternate routing schedules

Click one of the following links to connect with the type of information you want to view:

Panels	Tasks	Feature notes
"Routes" on page 260	"Grouping destination codes using a wild card" on page 251	
"Destination codes" on page 262	"Using the MCDN access codes to tandem calls" on page 257	
	"Programming the PRI routing table" on page 255	
	"Setting up a destination for local calling" on page 249	
	"Setting up a route through a dedicated trunk" on page 250	
	"Adding Carrier access codes to destination codes" on page 256	
"Alternate routes for routing schedules" on page 264	"Programming for least-cost routing" on page 252	
	"Using multiple routes and overflow routing" on page 252	

Panels	Tasks	Feature notes

See also:

- “Setting up VoIP trunks for fallback” on page 391
- “Configuring lines” on page 129
- “BRI ISDN: BRI T-loops” on page 195
- “Dialing plan: System settings” on page 267
- “Dialing plan: Public network” on page 275
- “Dialing plan: Private network settings” on page 281
- “Dialing plan: Line pools and line pool codes” on page 357
- “Public networking: Tandem calls from private node” on page 293
- “Private networking: Using destination codes” on page 339
- “Private networking: PRI and VoIP tandem networks” on page 323
- “Private networking: MCDN over PRI and VoIP” on page 297
- “Private networking: DPNSS network services (UK only)” on page 331
- “Configuring centralized voice mail” on page 351

Click the navigation tree heading to access general information about DN records.

Routes

The first step to setting up call routing is to define line pools into uniquely named routes. A route can be used with more than one destination code, but a line pool should only be used with one route.

Figure 81 illustrates the Routes tab.

Figure 81 Routes table

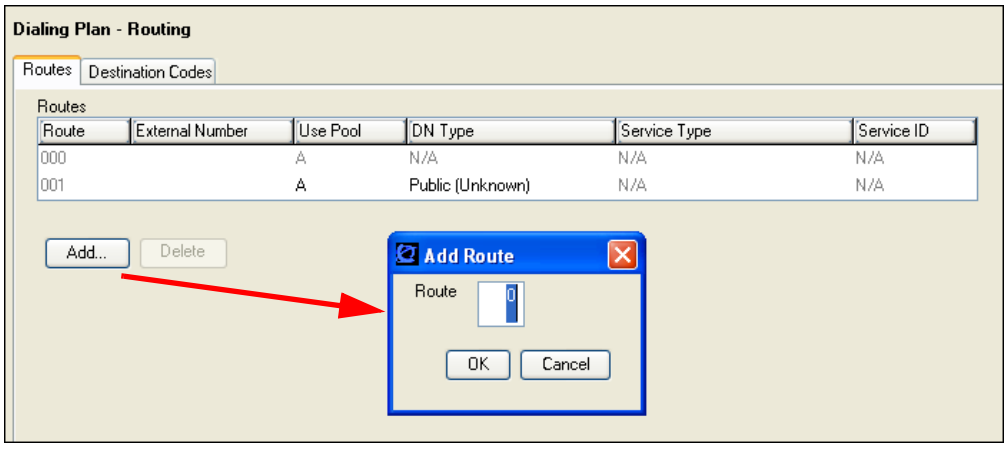


Table 47 describes the fields on the top panel.

Table 47 Route settings (Sheet 1 of 2)

Attribute	Value	Description
Route	<001-999>	This number is unique to each route.
External Number	<a maximum of 24 digits>	Enter the external or dial-out number for the route you want the assigned telephone to use. The external number is a digit or group of digits that get inserted in front of your dialed digits. If all the required numbers are defined in the destination code/dial string, this box can be left empty. Optional entries in the dial string: P = 1.5 second pause (counts as one digit in the dialing string) (F78 telset) DT = wait for dial tone (counts as two digits in the dialing string) (F804 telset)
Use Pool	Pool A to Pool O or BlocA to BlocF	Select a line pool for the route. The Bloc pools only display if you have PRI or VoIP trunks.
DN Type	Public Private Local (Subscriber) National Special (International)	This setting tells the system what type of line protocol the route uses to process the dial string. Refer to "PRI route types" on page 262. **MCDN private networks:** Local, National, and Special are special designators used to route calls from Meridian 1 systems, through BCM systems, out to the public network. Select **Configuration > Telephony > Dialing plan > Private Networks** tab to define the codes for these settings. Also refer to "Using the MCDN access codes to tandem calls" on page 257. When the BCM receives outgoing calls from the Meridian 1, it recognizes the call type and appends the appropriate access code to the Meridian dial string. This code then matches to a route that uses the same DN type, passing the call along, either to another node (the route would have the same DN type) or to the public network (the route would have a Public DN type), depending on the routing information.
Service Type	Public Private TIE Foreign exchange (FX) OUTWATS Switched Digital (SDS)	This setting tells the system what type of line protocol the route uses to process the dial string. These protocols are used for lines connected to DMS-100, DMS-250 and 4ESS switches. Refer to "PRI route types" on page 262.
Service ID	<digits>	If you choose a service, type in the identification number for the service.
Note:	**Outgoing call display:** If you have the trunks set up to send called number information, and the DN type is set to anything, except Private, the system sends the Public OLI number you specified under line programming. If the DN type is set to Private, the system sends the Private OLI number. Refer to "Line Access tab" in the *Device Configuration Guide* (NN40020-300).	

Table 47 Route settings (Sheet 2 of 2)

Attribute	Value	Description
Actions:		
Add	1. Under the routes table, click **Add**. 2. Enter a route number in the dialog box. 3. Click **OK** to save the new route.	
Delete	1. On the routes table, select the route you want to delete. 2. In the Routes pane, click **Delete.** 3. Click **OK**.	
Modifying routes:	**Warning:** Modifying some route settings may result in dropped calls. Ensure that you modify the destination codes Absorbed Length setting, if required, if you add or change the External Number entry. Changing the Use Pool or DN Types/Service Types values will result in dropped calls if the lines in the line pool do not support the DN/Service Type selected. 1. On the routes table, select the route you want to change. 2. Click the field you want to change for that route and enter the new value. 3. Press Tab on your keyboard to save the change.	

PRI route types

Table 48 lists the service/DN type choices available for PRI lines.

Table 48 PRI Service type/DN type values

PRI Protocol	Type	Values
SL-1	DN	Public, Private, Local, National, Special
ETSI Euro	DN	None, Overlap
ETSI QSIG	N/A	
NI	Service	Public, TIE, Foreign Exchange (FX), OUTWATS
DMS-100	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
DMS-250	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
4ESS	Service	TIE, OUTWATS, Switched Digital (SDS)

Destination codes

Once you have the routes configured, set up the dialing plan destination codes that allow users to access the routes. You can use a route for more than one destination code, as you may require different codes for the same route to define restrictions or special call designators.

Figure 82 illustrates the Destination codes panel.

Figure 82 Destination codes table panel

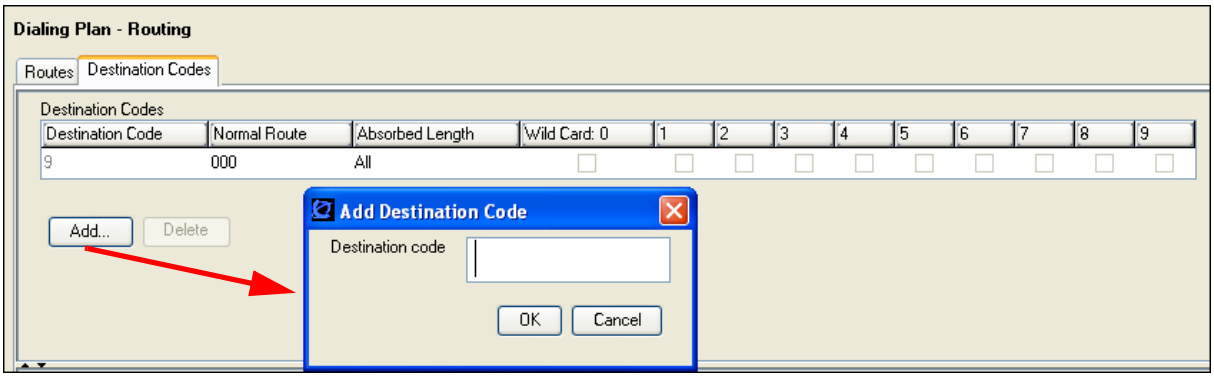


Table 49 describes the fields on the destination codes frame.

Table 49 Destination codes table

Attribute	Value	Description
Destination Code	<max. 12 digits>	This number precedes a telephone number to tell the system where the call needs to be routed. An *A* in the destination code represents an *any* character designation. The *A* code is a wildcard.
Normal Route	<configured route #>	This is the route that the system will use when the destination code is added to the dial string.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Wild Card 0 - 9	Included, Excluded, Unavailable	If you enter the wild card character *A* at the end of a destination code, then the following applies: Included: This number can be dialed as part of the destination code. Excluded: This number will not be accepted as part of a destination code string because it is already used in the system. Unavailable: This number is already defined in another destination code and cannot be used.
Actions		
Add	1. Under the Destination Codes table, click **Add**. 2. Enter the new destination code. 3. Click **OK** to save the route settings. 4. On the Destination Codes table, select the fields beside the route you just created, and modify them, as required. 5. Test the route.	
Delete	1. On the Destination Codes table, select the destination code you want to delete. 2. In the Destination Codes pane, click **Delete**. 3. Click **OK**.	

Note: The destination codes must not conflict with the following:

- park prefix
- external code
- direct dial digit
- Auto DN
- DISA DN
- Private access code
- line pool codes
- telephone DN
- public target line received digits
- other routing codes

Alternate routes for routing schedules

When you select a route on the Destination Codes panel, the alternate schedules for that route appear in a separate table. You only need to fill out this panel if your system is using routing schedules.

Note that in these schedules you can configure three routes. The second route acts as fallback route for the first route if it is unavailable. If the second route is also unavailable, the system will try the third route. The dialing sequence for these routes needs to be the same from the user perspective, as fallback occurs automatically and is not controlled by the user. If all three routes fail, the default normal route is used.

Figure 83 illustrates the Alternate Routes panel.

Figure 83 Alternate routing schedules

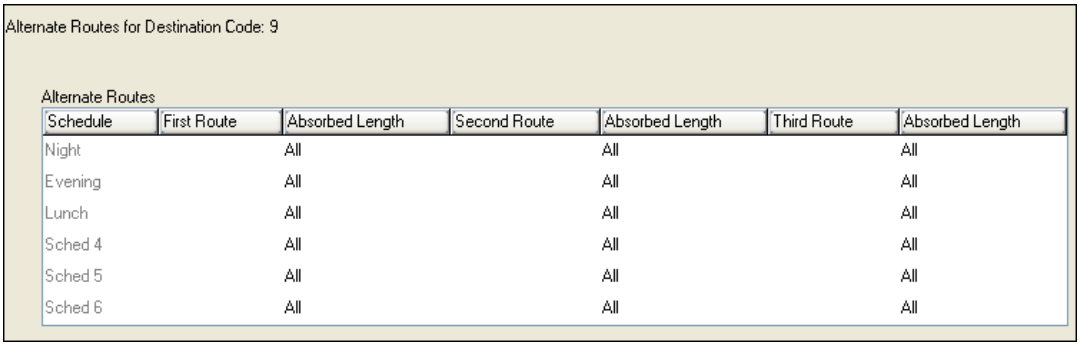


Table 50 describes the fields on the Destination codes frame.

Table 50 Destination codes schedules

Attribute	Value	Description
Schedule	Defaults: Night, Evening, Lunch, Weekend, Sched. 5, Sched. 6	If you use a different carrier at different times of the day or week, you can set the destination code to use that route and provide two more backup routes. The user does not experience any difference in dialing sequence.
First Route	<configured route #>	This is the route that the system will use, during the indicated schedule, when the destination code is added to the dial string.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Second Route	<configured route #>	This is the route the system will use if the first route is unavailable.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Third Route	<configured route #>	This is the route the system will use if the first and second route are unavailable.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.

Second Dial Tone

This feature provides dial tone for outgoing calls on any PRI line, based on the digits dialed. Digits dialed must match an entry in the second dial tone table to enable a second dial tone. Dial tone occurs on the line until another digit is dialed, a timeout occurs, or the user hangs up.

Up to 10 separate entries can be stored in the second dial tone table. The maximum digit length for each entry is four. Each entry must be unique and cannot conflict with:

- Internal DNs
- Hunt Group DNs
- DISA DNs
- Auto DNs
- Target Line DNs

Tips: Entries can match destination or access codes for outgoing lines.

The following paths indicate where to configure the Second Dial Tone in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Routing > Second Dial Tone**
- Telset interface: ****CONFIG > Services > Routing Service > 2nd Dial Tone**

Figure 84 Second Dial Tone

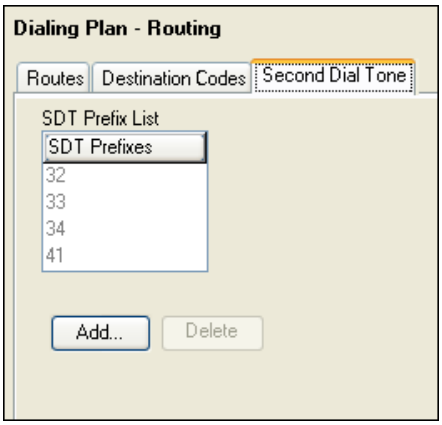


Table 2 Second Dial Tone

Attribute	Value	Description
SDT Prefix List		
SDT Prefixes		Enter the digits to match to trigger a second dial tone.
Actions		
Add	Button	Select to add an SDT prefix.
Delete	Button	Select an SDT prefix from the list and click delete to remove from the list.

Note: Second dial tone is not provided on outgoing lines for remote access users and for ISDN terminal users when the Call Transfer feature is activated.

Chapter 27
Dialing plan: System settings

The panels described in the following information define various common system settings that affect, or that are affected by, number planning.

The following paths indicate where to access system settings for dialing plans in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > General**
- Telset interface: ****CONFIG > System Programming > Access codes**; System Programming > General > Direct Dial sets

Panels/Subpanels	Tasks	Feature notes
"Common dialing plan settings" on page 267 • DN length • Dialing Time out • Park code • External code • Direct dial	"To define a direct dial set" on page 270 "Capabilities tab" in the *Device Configuration Guide* (NN40020-300)(assign direct dial set to a telephone)	"Configuring CLID on your system" on page 205 "DN length constraints" on page 270 "Received number notes" on page 271 "Tips about access codes" on page 272 "Call Park codes" on page 273
Also refer to: • "Dialing plan: Public network" on page 275 • "Dialing plan: Private network settings" on page 281 • "Dialing plan: Line pools and line pool codes" on page 357		
Click the navigation tree heading to access general information about dialing plans.		

Common dialing plan settings

The fields on the Dialing Plan - General panel allow you to set some general system dialing features.

Figure 85 illustrates the Dialing Plan - General panel.

Figure 85 Dialing Plan - General settings and Direct Dial devices

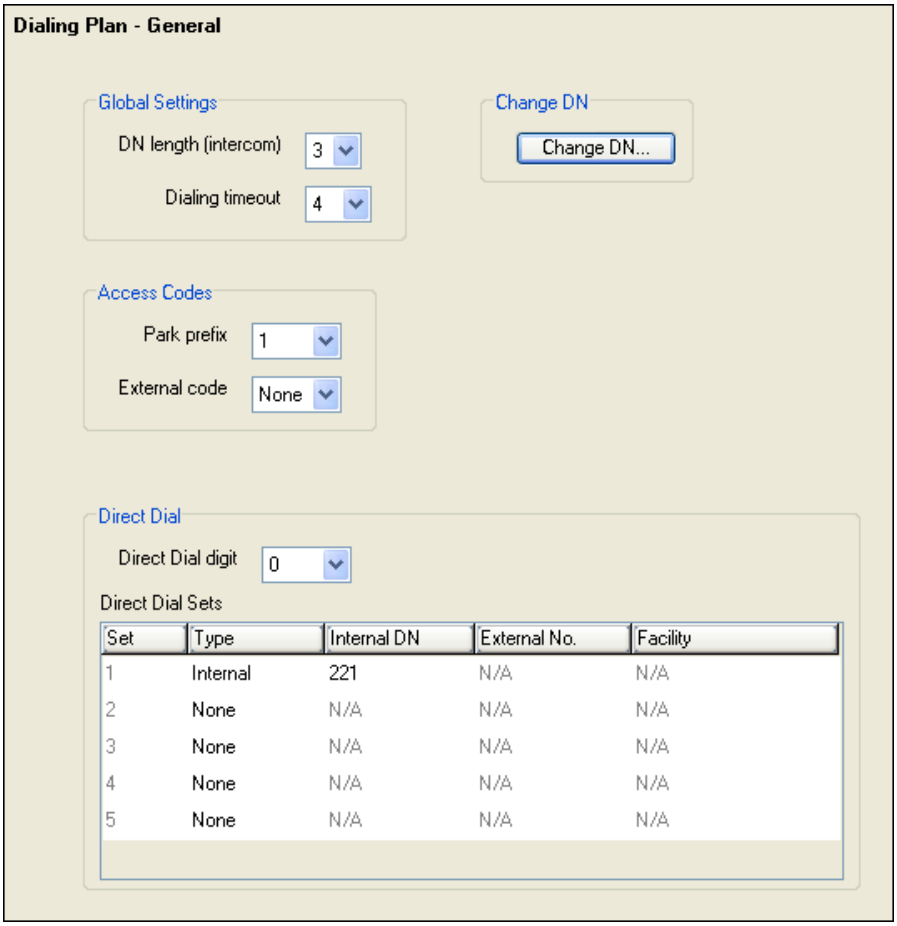


Table 51 describes each field on this panel.

Table 51 Private and Public received numbers (Sheet 1 of 3)

Attribute	Value	Description
Global Settings		
DN length (intercom)	(3 to 7)	This is the length of the locally dialed telephones. This field is set when the system is first configured. **Warning:** If this system is part of a private network, ensure that this value is compatible with the network requirements. This value is mirrored in the Private Received Number Length field for target lines. Refer to “Configuring lines: Target lines” on page 141. **Note:** If the DN length is changed, it will cause VM/CC to be defaulted in order to work properly.

Table 51 Private and Public received numbers (Sheet 2 of 3)

Attribute	Value	Description
Dialing timeout	Default: 4 seconds	This is the maximum period allowed between user dialpad presses before the system decides that the dial string is complete.
Access Codes		
Park prefix	None <one-digit number>	The Park prefix is the first digit of the call park retrieval code that a user enters to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked. Refer to "Call Park codes" on page 273 before choosing a number. **SWCA note:** If this field is set to **None**, the system-wide call appearance (SWCA) feature will not work. Refer to "System Wide Call Appearances" in the *Device Configuration Guide* (NN40020-300).
External code	None <one-digit number>	The External code setting allows you to assign the external line access code for 7100 and 7000 digital phones and analog telephones attached to ATA 2s or to analog modules to access external lines. **Note:** Model 7000 phones are supported in Europe only. When the caller picks up the handset, the system tone sounds. The caller then enters this number to access an external line. **Note:** This number is overridden by line pool or starting with the same digit(s). Refer to "Tips about access codes" on page 272 before choosing a number.
Change DN		
Change DN	<button>	Click to reidentify a DN. **Note**: This method is faster than reidentifying the DNs under **Configuration > Telephony > Dialing Plan > DNs**
Direct Dial		
Direct Dial digit	None <one-digit number>	The Direct dial digit setting allows you to specify a single system-wide digit to call a direct dial telephone.
Define Direct Dial Sets: Refer to "To define a direct dial set" on page 270.		
Set	<1-5>	This tags the telephone to the system.
Type	Internal External None	This is the type of number for the direct-dial set.
Internal DN	DN	The DN number of the telephone to be designated as the direct dial set. (Internal sets).
External No.	<external dial string>	The actual phone number, including destination codes, of the direct dial set (External sets).

Table 51 Private and Public received numbers (Sheet 3 of 3)

Attribute	Value	Description
Facility	Line Pool (A-O) Use prime line Use routing table	The facility to be used to route the call to a direct dial set that you define with an external number. **Note:** If you choose **Use prime line**, ensure that prime line is not assigned to the intercom button*s* for your telephones. When prime line is assigned as an intercom button, it chooses the first available line pool assigned to the telephone to make a call. If this line pool does not have the correct lines for routing the call, the direct dial call will fail. Refer to "Line Access tab" in the *Device Configuration Guide* (NN40020-300).

To define a direct dial set

1. On the Direct Dial table, click the fields beside the set number you want to configure and enter the appropriate values.
2. Press Tab on your keyboard to save the values.
3. Go to the DN records of the telephones where you want the direct dial set assigned and assign the set under "Preferences tab" in the *Device Configuration Guide* (NN40020-300).

Note: The BCM cannot verify that the number you assign as an external direct dial set is valid. Check the number before assigning it as a direct dial set by calling the direct dial you have assigned.

Configuration notes and tips

The following information expands on some of the fields on the tabs on the Dialing Plan - General panel.

- "DN length constraints" on page 270
- "Received number notes" on page 271
- "Tips about access codes" on page 272
- "Call Park codes" on page 273

DN length constraints

Warning: Do not change DN length immediately after a system startup. You must wait until the system is operational with two solid green status LEDs.

Warning: Increasing the DN length affects other areas of the system:

If the DN length change creates a conflict with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code changes to None, and the corresponding feature is disabled.

Optional applications affected by DN length changes:

Voice mail and **Contact Center** applications are reset if you change the DN length after these services are installed.

Warning: If your system is running with a PBX telephony template, the Public and Private received number length are set to 3 (digits) at start-up. Increasing the DN length after system startup does not change these digits, so you will need to manually change the Public and Private received number length.

Private OLIs are automatically assigned to the DN records if the DN length and the Private received number length are the same. If this changes, the Private OLIs are cleared, or are not assigned (PBX template).

Network note: If your system is part of a private network, ensure that you confirm the dialing plan for the network before changing this length. If you change the length, ensure that you check all DN-related settings after the change.

Received number notes

- If you change the received number length for your system, the **Public number** entry for the target lines will clear if the new received # length is less than the number entered in this field.
- If the new received number length has more digits than the number entered in the target lines Public Number field, the entry remains, but does not update to the new DN length.
- A private OLI is automatically assigned to the DNs if the DN length and the Received number length are the same. If either changes so that they are not the same, the private OLI field is cleared or not assigned (PBX template).

Tips about access codes

Here are some pointers to assist you in planning the access codes for your system.

Note: The following values must not conflict:

- Park prefix
- external code
- direct dial digit
- Private access code
- Public/Private Auto DN
- Public/Private DISA DN
- line pool code/destination code
- telephone DN

Note: If the line pool code and the external code start with the same digit, the line pool code programming supersedes the external code.

External line access code:

Example: If you enter the following selections:

Park Prefix - 1

Direct Dial digit - 0

Telephone DNs - 2000-2500

You wish to add a destination code of 2500 and 12. This cannot be accomplished as this would conflict with existing dialing numbers. To solve this you could modify the Park prefix and change the Telephone DN of 2500.

- If the DN length is changed, and the changed DNs conflict with the external line access code, the setting changes to None.
- **Direct dial telephone:** Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming.

  If the DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.
- **Public/Private Auto DN:** The length of the Auto DNs are the same as the Public or Private Received Number Lengths specified under **Configuration > Telephony > Dialing Plan > Public or Private**. The public/private Auto DN is cleared if the corresponding Received Number Length is changed.

- **Public/Private DISA DN:** The length of the DISA DNs are the same as the Public or Private Received number length specified under **Configuration > Telephony > Dialing Plan > Public or Private**. The public/private DISA DN is cleared if the corresponding Received number length is changed.

Call Park codes

When you park a call (**FEATURE 74**), the system assigns one of 25 codes for the retrieval of the call. You can then press the Page display key to announce the code that appears on the display.

These three-digit codes include the Call Park prefix, which can be any digit from 1 to 9, and a two-digit call number between 01 and 25. For example, if the Call Park prefix is 1, the first parked call is assigned Call Park retrieval code 101.

Note: The park prefix must not conflict with the following:

- park prefix
- external code
- Direct dial digit
- Private access code
- Public/Private Auto DN
- Public/Private DISA DN
- line pool code/destination code
- telephone DN

Note: Other programmable settings may affect what numbers appear in the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes.
If the DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

The system assigns Call Park codes to calls in sequence, from the lowest to the highest, until all the codes are used. A round-robin method means the use of different of codes ensures a call reaches the right person, especially when more than one incoming call is parked.

The highest call number (the Call Park prefix followed by 25) is used by model 7000 and 7100 telephones, analog telephones, or devices connected to the system using an ATA2. Analog telephones or devices cannot use the other Call Park codes.

Note: Model 7000 phones are supported in Europe only.

Calls are retrieved by pressing the intercom button and dialing the retrieval code. On model 7000 and analog telephones, pick up the receiver, and then dial ***<parkcode>*25**.

You also need to program the delay timer that determines when external parked calls that are not answered return to the originating telephone. Refer to “Timers” in the *Device Configuration Guide* (NN40020-300).

You can disable Call Park by setting the Park Code to None.

Chapter 28
Dialing plan: Public network

The panel described in the following information defines the number planning required for calls exiting the system to the public telephone network.

The following paths indicate where to access the dialing plan for public network in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Public Network**
- Telset interface: ****CONFIG > System Prgrming > Dialing Plan > Public Network**

Panels/Subpanels	Tasks	Feature notes
"Public dialing plan settings" on page 275		
"Public Network Settings" on page 276		
"Public network DN lengths" on page 277	"Adding a DN Prefix for public dialing" on page 278 "Modifying a DN prefix" on page 278 "Deleting a DN prefix" on page 279	"Outgoing public calls routing" on page 279
"Carrier Codes" on page 279	"Adding a carrier code" on page 280 "Modifying a carrier code" on page 280 "Deleting a carrier code" on page 280	

"Configuration notes and tips" on page 270

See also:

- "Dialing plan: System settings" on page 267
- "Dialing plan: Private network settings" on page 281
- "Public networking: Setting up basic systems" on page 289

Click the navigation tree heading to access general information about dialing plans.

Public dialing plan settings

The Dialing Plan - Public Network panel displays the fields that determine dialing information specific to dialing in or out to a public network from the host system.

This panel includes information about:

- "Public Network Settings" on page 276
- "Public network DN lengths" on page 277
- "Carrier Codes" on page 279

Public Network Settings

This following describes system settings that allow the system to determine if an incoming call is meant for the local system. These settings determine how many digits the system needs to receive before sending the dial string over the trunk interface.

Figure 86 illustrates the Public Network Settings panel.

Figure 86 Public Network Settings panel

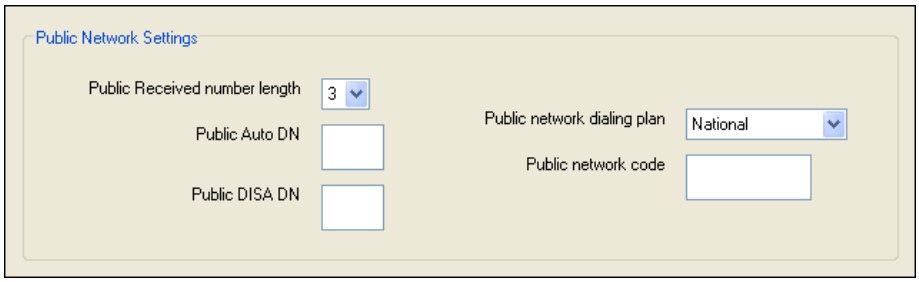


Table 52 describes each field in the Public Network Settings box.

Table 52 Private and Public received numbers (Sheet 1 of 2)

Attribute	Value	Description
Public Received number length (max)	<2-12>	The maximum number of digits (2, 3, 4, 5, 6, 7) that the system uses to determine if an incoming call tagged as public fits the system public DN numbering. Default: DID template, same as DN length; PBX template: 3 Also refer to "Setting up a destination for local calling" on page 249.
Public Auto DN	<DN digits to be received from the auto-answer trunk>	Public network calls answered without DISA require no password to access the BCM. The type of service that applies to the call depends on the restrictions assigned to the trunk.
Public DISA DN	<DISA DN digits to be received from the auto-answer trunk>	For public network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (CoS) that applies to the call is determined by this CoS password. After a remote user accesses the BCM, they can change the existing CoS using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate CoS passwords with different dialing out privileges for individuals.

Table 52 Private and Public received numbers (Sheet 2 of 2)

Attribute	Value	Description
Public network dialing plan	National Local (Subscriber)	Local dialing plan defines a seven-digit numbering scheme. National dialing plans define an extended number scheme. North America is set to 10 digits. However, systems in other countries may have a variable length.
Public network code	<1 to 7 digits>	This number concatenates with the Public OLI, which, by default, is the DN of the device. **Note**: In systems running the North American profile, if the Public OLI contains the public network code, that entry overrides any entry in this field. Refer to “Line Access tab” in the *Device Configuration Guide* (NN40020-300).

Public network DN lengths

The Public network DN length tells the system how long dialing strings will be when entering the network. For example, if you dial 18005551212 the public network DN length for 1, which is 11, tells the system to wait until 11 digits are entered before processing the call.

Note: If the values for Public Network DN length are set too short, digits will be stripped from the dialing string. Conversely, if the values are set too large, the dialing will take longer to process.

The Public Network DN Lengths/Carrier Codes panel allows you to define DN prefixes and define the length of the prefixes for public dialing. Figure 87 illustrates this panel.

Figure 87 Public Network DN Lengths/Carrier Codes panels

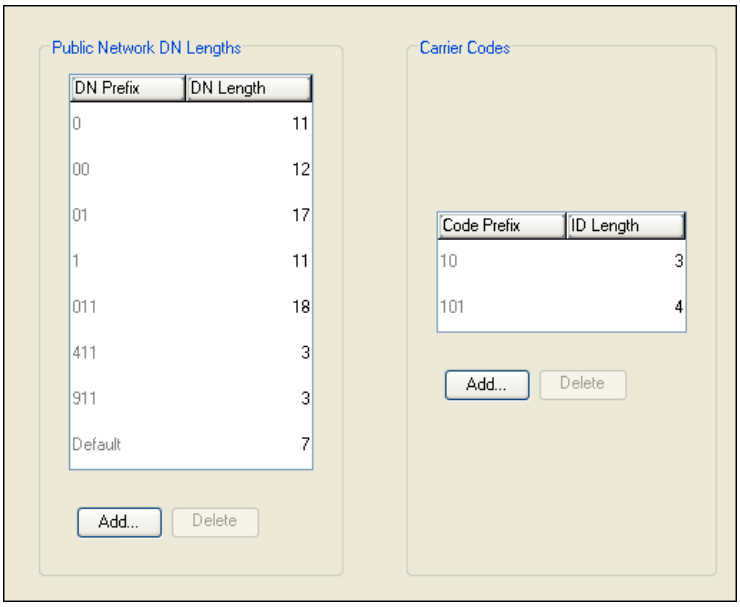


Table 53 describes each field on this panel.

Table 53 Public network DN values

Attribute	Values	Description
DN Prefix	<XXXX>	This is the number that must precede a dial string exiting the system to the public network. Each prefix defines a specific destination or type of call.
DN Length	<1-25>	This number indicates how many numbers, starting from the front of the dial string, the system will wait before sending to the public network.

About the Public Network DN lengths table

In the public Network DN lengths table:

- You can define up to 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 - 25).
- Several entries are predefined in the North America profile. These defaults can handle most regions in North America without the need for additional programming. If required, you can remove or modify these entries.
- The table always contains one default entry. You cannot remove this entry. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

Adding a DN Prefix for public dialing

The Default DN prefix cannot be deleted. The DN length for this prefix varies, depending on the country profile running on the system.

To add a new Prefix, follow these steps.

1. In the Public Network DN Lengths box, click **Add**.
2. Enter the new parameters:
   - DN Prefix
   - DN Length
3. Click **Save**.

Modifying a DN prefix

You can only change the DN length for a prefix. To change the prefix itself, delete the existing prefix and enter a new one.

1. On the Public Network DN Lengths panel, click the DN prefix you want to modify.
2. Click in the DN length field for that prefix and enter the new value.

Deleting a DN prefix

Note: Dialing prefixes are used system-wide for users to make calls. Delete prefixes with caution.

1 On the Public Network DN Lengths panel, click the DN prefix you want to delete.

2 Click **Delete**.

3 Click **OK** on the confirmation dialog.

Outgoing public calls routing

Outgoing public calls from within the system typically have the routes set to Public. Refer to "Setting up a destination for local calling" on page 249. The NPI/TON gets sent as Unknown/ Unknown. The public called number length is based on the Public DN lengths table in the Public networks dialing plan.

MCDN trunks also allow public call types when tandeming calls from another system on the private network. Some of these systems use specific call types that the BCM needs to recognize to pass on correctly. Also refer to "Using the MCDN access codes to tandem calls" on page 257.

Type of call	NPI/TON	BCM prepend access code	BCM monitor display
Local	E164/Local	Local access code (9)	E.164/Subscriber
National	E164/National	National access code (X1)	E.164/National
Special calls (international, 911, etc.)	Private/Special	Special access code (9)	

Carrier Codes

The Carrier Codes table allows you to enter a maximum of five carrier code prefixes.

- You can define up to five carrier codes.
- Entries may be predefined for a specific country profile, but you can remove these defaults.
- Each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 to 9).
- Each entry is identified by the prefix digits themselves.

Table 54 describes each field on this panel.

Table 54 Carrier Code values

Attribute	Values	Description
Code Prefix	<one to six digits> (Read-only)	This value defines the prefix that will be used to access the carrier code.
ID Length	1, 2, 3, 4, 5, 6, 7, 8, or 9	This value defines the carrier ID length.

Adding a carrier code

1. Click **Add**.
2. Enter the required code and ID:
   - Code Prefix
   - ID length
3. Click **Save**.

Modifying a carrier code

1. Click the line for the Carrier Code where you want to change information.
2. Click the field that you want to change, and enter the new value.

Deleting a carrier code

1. Click the line for the carrier code that you want to delete.
2. Click **Delete**.
3. Click **OK**.

Chapter 29
Dialing plan: Private network settings

The panels described in the following information define various system settings that affect or that are affected by number planning for private networks.

The following paths indicate where to access the dialing plan for private networks in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Private Network**
- Telset interface: ****CONFIG > System Prgrming > Dialing Plan > Private Network**

Panels/Subpanels	Tasks/Features
"Private Network dialing plan settings" on page 281 "Private Network Settings" on page 282 "Private Network - MCDN network (PRI SL-1, PRI ETSI, VoIP)" on page 284 "ETSI-specific network features" on page 286	"Outgoing private calls routing" on page 287
"Configuration notes and tips" on page 270	
Also refer to: • "Dialing plan: System settings" on page 267 • "Dialing plan: Public network" on page 275 • "Private networking: Basic parameters" on page 315 • "Private networking: Using destination codes" on page 339 • "Private networking: PRI Call-by-Call services" on page 343 • "Private networking: PRI and VoIP tandem networks" on page 323 • "Private networking: MCDN over PRI and VoIP" on page 297 • "Private networking: MCDN and ETSI network features" on page 319 • "Private networking: DPNSS network services (UK only)" on page 331	
Click the navigation tree heading to access general information about dialing plans.	

Private Network dialing plan settings

The boxes on the Private Network Settings panel have fields that apply specifically to private network configurations. Network configurations can be set up between BCM systems, between BCM systems and other call servers such as the Business Communications Manager, Meridian 1, or Succession 1000.

Some of the settings on this panel also depend on the market profile of the system.

- "Private Network Settings" on page 282

- "Private Network - MCDN network (PRI SL-1, PRI ETSI, VoIP)" on page 284
- "ETSI-specific network features" on page 286

Private Network Settings

The settings on the Private Network Settings panel describe the numbering that the system uses to assess an incoming call to determine if the call is destined for your system or needs to be routed elsewhere on the private or public network. This panel is illustrated in Figure 88.

Note: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using "1" as an access code in a private network, conflicts with the PSTN numbering plan for long distance calls.

Figure 88 Private Network Settings panel

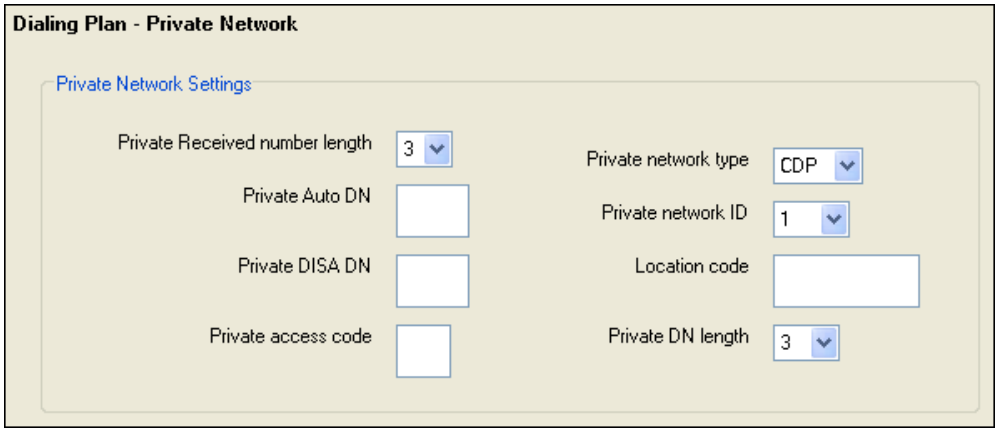


Table 55 describes each field on this panel.

Table 55 Private Network Settings (Sheet 1 of 2)

Attribute	Value	Description
Private Network Settings		
Private Received number length	2, 3, 4, 5, 6, 7	The number of digits of an incoming dial string that the system uses to determine if a call tagged as Private fits the system private DN numbering. Default: DID template, same as DN length; PBX template: 3
* Private Auto DN	Digits to be received from a private auto-answer trunk>	Private network calls answered without DISA require no password to access the BCM. The type of service that applies to the call depends on the restrictions assigned to the trunk.

Table 55 Private Network Settings (Sheet 2 of 2)

Attribute	Value	Description
* Private DISA DN	<DISA DN digits to be received from the auto-answer trunk>	For private network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (CoS) that applies to the call is determined by this CoS password. After a remote user accesses the BCM, they can change the existing CoS password using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate CoS passwords with different dialing out privileges for individuals.
Private access code	<systemcode> **MCDN:** coordinate with National access code	This code identifies this system to the private network. It comes in as the first digit in a dial string defined as private and is read based on the private DN length. Example: if the dialed number is 7880, and the private DN length is 4, the system scans the four digits from the right, recognizing the 7 as the private access code for this system.
Private network type	CDP, UDP, None	You can specify if your Private network uses a coordinated dialing plan (CDP) or a universal dialing plan (UDP). If you choose None, the private networking supplementary services are not available.
Private Network ID (CDP/UDP networks)	<1-127>	This is the unique number that identifies the system to the Meridian PRI-MCDN network. Both end points must match on a PRI-MCDN network. On a VoIP trunking-MCDN network, this ID must be the same on all nodes. This number is supplied by the private network administrator.
Location code	<up to seven digits>	This code identifies this particular system for calls within the network for a UDP dialing plan. This number must be unique. **Note**: The system uses the Private Access Code length, plus the Location code length, plus the DN length to determine the DN length required to determine that a call is a private network call.
*Private DN length	3-14	The Private DN length parameter specifies the length of a dial string that the system uses to determine that the call is a private network call, when the route uses DN Type: Private.
* CDP and UDP private DN lengths are determined this way: CDP: the system uses the telephone DN length UDP: the system combines the private access code length + location code length + telephone DN length. When a call comes in, the system recognizes the leading digits as a private call and removes (truncates) them, leaving the telephone DN, which is recognized as the private DN length.		

Note: The value entered for **Private Access Code** should be a local digit different than the digits used as Destination Codes in **Configuration > Telephony > Dialing Plan > Routing > Destination Codes**. This field should not be blank. For example, if there are routes that use 9 and 6 as Destination Codes, a good value for this field could be 1, 2, 3, 4, 5, 7, or 8. Using a blank value, or 9 or 6, will cause a Fail of the call reason "Reject".

Private Network - MCDN network (PRI SL-1, PRI ETSI, VoIP)

If your system is part of a private network using the MCDN protocol, you may need to configure these special dialing access codes and network settings.

Figure 89 illustrates the MCDN panel.

Figure 89 MCDN network values

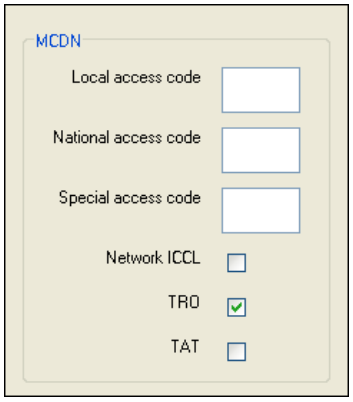


Table 56 describes the values for these fields.

Table 56 Private network values (Sheet 1 of 2)

Attribute	Values	Description
Private networking also provides access to tandem calling and toll bypass functionality to users calling into the system. For example, a PSTN user in Toronto could call a PSTN user in Ottawa and have the call routed over the private network connection from the Toronto office to the Ottawa office and then out to the PSTN from the Ottawa office. This bypasses any long distance toll charges. BCM to BCM to PSTN: Calls are routed as private over the private network and then flagged as public to go out to the end node PSTN. Meridian to BCM to PSTN: Special call codes from the Meridian (Local, National, and Special access codes) need to be recognized by the BCM and correctly passed to the local PSTN.		

Table 56 Private network values (Sheet 2 of 2)

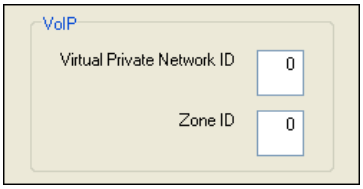
Local access code	<code to access local PSTN>	MCDN connections only. This number is prepended to an incoming M1 local dial string and designates the call as a Local call type (typically 9). Refer to "Using the MCDN access codes to tandem calls" on page 257.
National access code	<private access code + 1>	MCDN connections only. This number is prepended to an incoming call marked as a long distance call, and designates the call as a National type call (private access code + 1).
Special access code	<code to access local PSTN>	MCDN connections only. This number is prepended to an incoming international (011....) or special-case dial string (911, 411) and designates the call as a special type call (9011...., 9911, 9411).
Incoming and tandem calls (Also refer to "Dialing plan: Routing and destination codes" on page 259**).**		
Network ICCL	<check box>	ISDN Call Connection Limitation is part of the call initiation request. This feature acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.
TRO	<check box>	Trunk Route Optimization occurs during the call setup. This feature finds the most direct route through the network to send a call between nodes.
TAT	<check box>	Trunk anti-tromboning works during an active call to find the optimum routing.
These features require compatible programming on the remote system.		

VoIP-specific private network dialing

The features contained in the VoIP subpanel are required for installations like the Survivable Remote Gateway (SRG), where the remote call server requires bandwidth management to handle calls.

Figure 90 illustrates the VoIP panel.

Figure 90 VoIP special dialing plan settings



Use Table 57 to determine the settings you want to define network services feature availability.

Table 57 VoIP special dialing plan values

Attribute	Values	Description

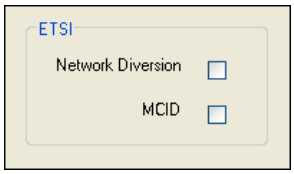
Table 57 VoIP special dialing plan values

Virtual Private Network ID	<digits>	Default: 0 This is the VPN ID for a remote system, such as Succession 1000/M. In some applications, such as for the Survivable Remote Gateway (SRG) acting as a Branch Office, this ID is required to ensure that Bandwidth Management is handled correctly for calls coming into the Succession 1000/M from your system. See "VPN overview" on page 525 for more information on VPN.
Zone ID	<digits>	Default:0 A remote system, such as Succession 1000/M, may configure your system into a separate zone to accommodate specific dialing requirements, such as for an SRG system acting as a Branch Office to a Succession 1000/M system. The system administrator of the Succession 1000/M system provides the Zone ID. Enter that number here and include it in any destination codes directed to, or through, that system so that the remote system can correctly direct incoming calls.

ETSI-specific network features

The features contained in the ETSI subpanel are service provider-based network services available for some PRI-ETSI lines. This subpanel is illustrated in Figure 91.

Figure 91 ETSI private network settings



Use Table 58 to determine the settings you want to define network services feature availability.

Table 58 ETSI, MCDN, and VoIP trunk private network settings fields

Attribute	Values	Description
Network Diversion	<check box>	Allows you to choose if you want to allow calls to be redirected to an outside network.
MCID	<check box>	If you select this check box, the called party can use **FEATURE 897** to request the service provider network to record the identity of an incoming call. Including: • called party number • calling party number • local time and date of the activity • calling party sub-address, if provided by the calling user

Table 58 ETSI, MCDN, and VoIP trunk private network settings fields (Continued)

Attribute	Values	Description
	MCID note:	The feature code must be entered within 25 seconds of the caller hanging up (a 25-second busy tone occurs). If the called party hangs up first, there is no opportunity to use the feature. **Note**: The call identification comes from your service provider, not the local system. You must have the service activated by the CO before the feature is active for the user, regardless of the setting in this field.

Outgoing private calls routing

When you set up routing for private calls, the route is set to Private. Refer to "Setting up a route through a dedicated trunk" on page 250.

How the system identifies the call depends on the type of trunk chosen for the route. Refer to the table below.

Dialing plan setting	NPI/TON	Private called number length based on
MCDN trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/UDP	private access code + home location code (LOC) + private received digits
CDP	Private/CDP	private received digit
DMS-100/DMS-250/ETSI-QSIG trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/Subscriber	private access code + home location code (LOC) + private received digits
CDP	Private/Subscriber	private received digit

Chapter 30
Public networking: Setting up basic systems

Public networks are the connection between the BCM and the public network (PSTN network).

This following provides examples of two basic types of systems.

- "Public networks: PBX system setup" on page 289
- "Public network: DID system" on page 290

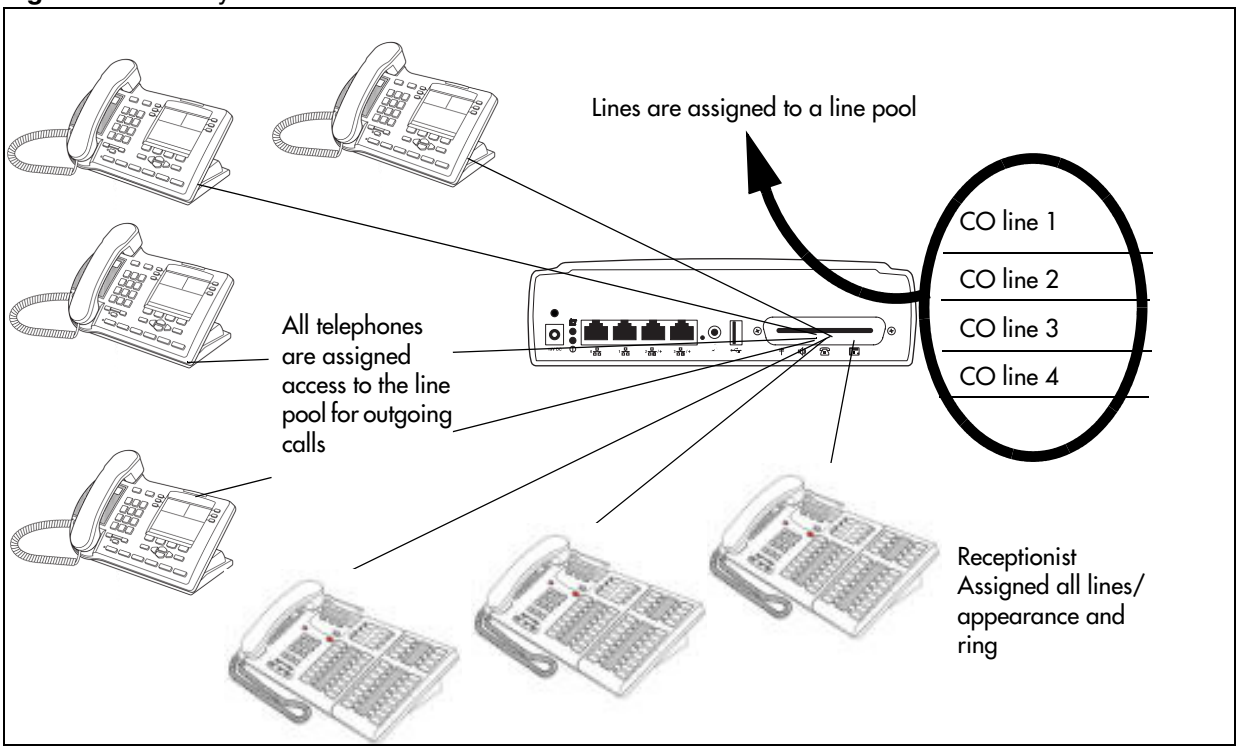
Public networks: PBX system setup

PBX is Short for Private Branch Exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX. Dialing within the PBX is typically 3 to 4 digit dialing between local and remote networked nodes.

This setup is for a larger offices which have fewer CO lines than there are telephones. In this case the lines are pooled, and the line pool is assigned to all telephones. As well, there is a designated attendant with a telephone that has all lines individually assigned.

Figure 92 illustrates an example of a PBX system.

Figure 92 PBX system


Lines are assigned to a line pool
CO line 1
CO line 2
CO line 3
CO line 4
All telephones are assigned access to the line pool for outgoing calls
Receptionist Assigned all lines/ appearance and ring

Programming:

Lines

- Set lines to manual answer.
- Configure into a line pool.

Telephones

- Line pools are assigned to general office telephones.
- The Prime line is set to the line pool.
- Lines are assigned individually and as a line pool to the central answer position (set to appear and ring).

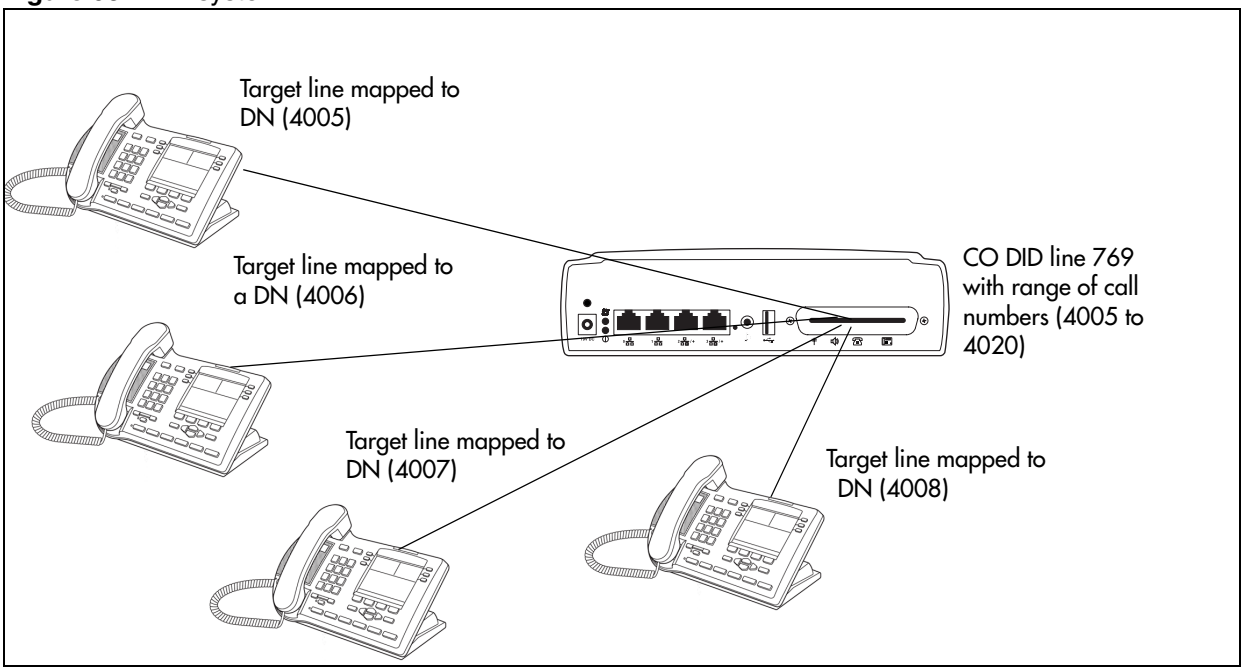
Public network: DID system

Direct Inward Dialing (DID): A call is received over the DID circuit (for example, PRI) and is preceded by a packet of information (Receive Digits) containing the number that was dialed. The BCM decodes this information and routes the call to the extension that has been programmed with the designated Target Line. The benefit to the customer is a pooled access group for incoming calls so that dedicated lines are not required to be terminated on the system for each user.

This setup allows you to assign a dedicated phone number to each telephone. The CO assigns a list of available numbers for each DID line. You can change your DN range to match these numbers, or you can use target lines to match each number with a DN.

Figure 93 illustrates an example of a DID system.

Figure 93 DID system



Programming:

Lines

- Assign lines as auto-answer. Note: DID lines are incoming only. PRI lines can be used for both directions.
- Configure target lines for each telephone, indicating public received number (769-4006 in the example above).

Routing

- Create line pool access code to outgoing line pool.

Telephones

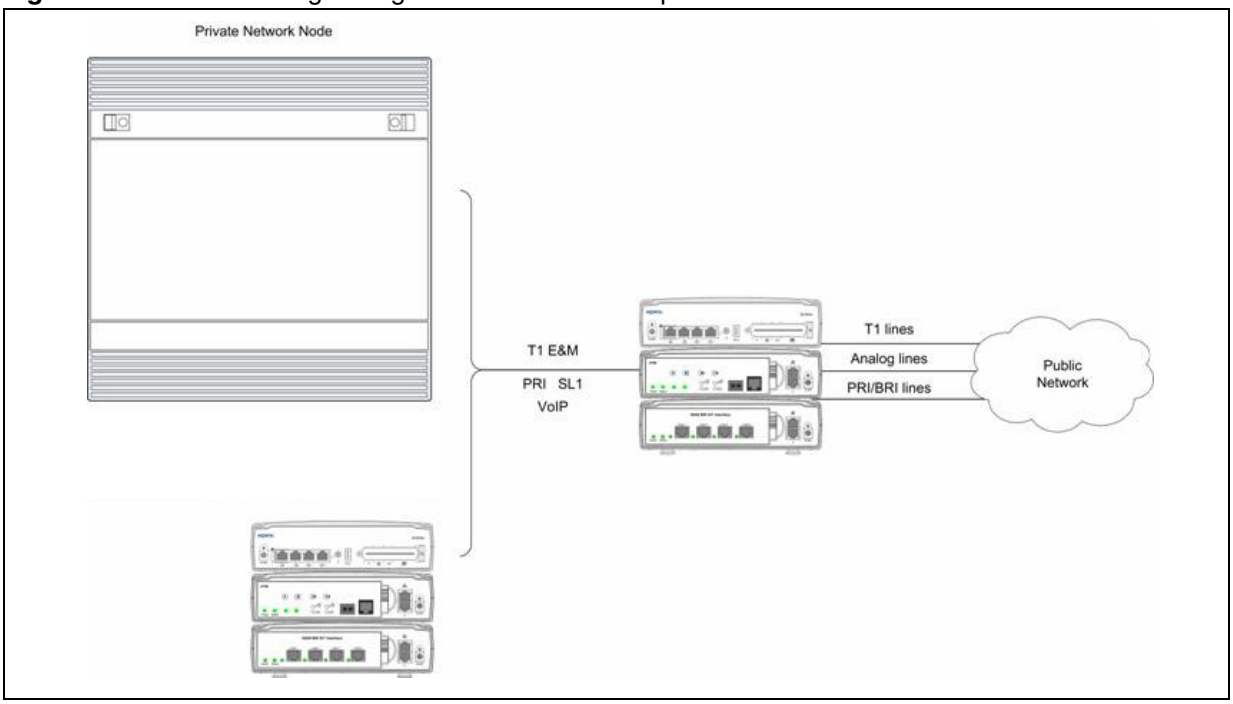
- Assign target line to each telephone.
- Assign outgoing line pool to telephones.
- Set call forward no answer and call forward on busy to attendant or voice mail system, if available.

Chapter 31
Public networking: Tandem calls from private node

If your system is connected by a private network to another system that does not have PSTN line access, or which is not located within the local dialing range, you can set up a routing plan that allows the users of the private network to dial into your system, and through your system to the PSTN network. This type of call feature is referred to as tandem dialing. Refer to "Programming for tandem dialing" on page 293.

The reverse is also true. You can set up routing so that calls from the PSTN can be passed through your system and over the private network to the remote node. Also refer to "Private networking: PRI and VoIP tandem networks" on page 323.

Figure 94 Tandem dialing through a BCM to or from a private network



Programming for tandem dialing

Since incoming lines terminate within the system, you need to set up routing to pass the calls along to the required destination.

Lines:

- Set up private network lines as auto answer (if applicable).
- Put private and public lines into separate line pools.
- Assign lines to configured Remote Access Packages.

Dialing plan/Routing:

- Coordinate Dialing plan with private network node.
- Assign each line pool to a route
- Create destination codes for the private network node, and the public network, using the appropriate routes. On public route, drop the public network access code off the dial string. On the private route, drop the private network access code off the dial string.

Telephones:

- System telephones are not involved in tandem transactions. However, for calls destined for the system, ensure that the telephones have the appropriate line/line pool assignments to receive calls from both the public and private networks.

Caller access on a tandem network

In this type of configuration, there are three types of callers:

Each type of caller has a specific method of accessing the other two systems.

Callers using BCM

These callers can:

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network
- select an outgoing central office line to access the public network
- use all of the BCM features

Callers in the public network

These callers use the public lines to:

- call directly to one or more BCM telephones
- call into BCM and select an outgoing TIE line to access a private network
- call into BCM and select an outgoing central office line to access the public network
- call into BCM and use remote features

Callers in the private network node

These callers use private lines to:

- call directly to one or more BCM telephones
- call into BCM and select an outgoing TIE line to access other nodes in a private network
- call into BCM and select an outgoing central office line to access the public network
- call into BCM and use remote features

Chapter 32
Private networking: MCDN over PRI and VoIP

The following describes how to network BCMs together in a private network using PRI lines with MCDN protocol. When BCMs are networked with other call services, such as Meridian 1, using the MCDN protocol, the network can also support centralized voice mail.

This chapter discusses MCDN networking based on North American trunks (PRI SL-1). ETSI-QSIG private networking is configured very similarly, although network features may be supported slightly differently.

The following describes the different aspects of MCDN private networking.

- "Using MCDN to network with a Meridian system" on page 297
- "Configuring fallback over a VoIP MCDN network" on page 311
- "Networking with ETSI QSIG" on page 313

Refer to "Private networking: Basic parameters" on page 315 for general requirements and directions for setting up non-PRI private networks.

Using MCDN to network with a Meridian system

When you connect your BCM systems through the MCDN protocol to a Meridian 1, the Meridian system manages several aspects of the network, including voice mail, auto attendant services, and system timing.

Programming note: For information about networking voice over IP (VoIP) trunks, which also can be set to use MCDN. For networks running BCM 1.0 software or newer, the trunk protocol for Meridian 1 IPT connection should be set to CSE.

The following information includes how to set up an MCDN network:

- "Meridian system requirements"
- "MCDN networking checklist" on page 303

For an example of an MCDN system and the BCM programming to support it, refer to "An example of a private network with Meridian 1" on page 307.

Meridian system requirements

When setting up networking with Meridian, the Meridian systems must provide the following:

- provide the correct software version to allow MCDN features. If your Meridian system administrator cannot confirm this, call your technical support center (TSC) or 1-800-4NORTEL.

The Meridian must provide the following:

- end-to-end signaling (option 10)
- message center (option 46) and an IVMS link (option 35)
- Meridian Mail link (options 77 and 85)
- basic Attendant Console Directory features (options 40, 45, and 83)
- ISDN PRI or ISDN Signaling link (options 145 and 146 or 145 and 147)
- advanced ISDN features (option 148)
- network message services (option 175)

- act as the timing master for the private network connections
- use descending mode for PRI B-channel selection
- recognize dial codes for all nodes in the network
- provide routing tables that direct incoming calls to the correct nodes on the network, including DID calls from the public network
- recognize the destination code (usually 9) that indicates a public network call, regardless of where in the network the number was dialed from

Note: For MCDN over VoIP trunks, the Meridian uses the IPT trunk card. Both systems must have remote gateways pointed to correct system types and protocols. Refer to "Configuring VoIP trunk gateways" on page 381 for information about Remote Gateways for the BCM system.

Software requirements

These additional software packages may be required to activate all the options on the Meridian.

For a new M1 (option 81C, 61C or 51C) on X11 Rls 25, the following additional packages are required to provide the software options listed above:

- SW0059B
- SW0052D
- SW0221C
- SW0051B

For a new M1 Option 11C or 11C Mini or X11 Rel. 25, order one of the following:

- Enterprise software package
- NAS/VNS software package

Meridian MCDN call features over PRI SL-1 lines

Besides the general MCDN features described in "Using the MCDN access codes to tandem calls" on page 257, an MCDN connection with a Meridian 1 voice mail system also provides some special call features, which are listed in Table 59.

Table 59 MCDN feature enhancements

Centralized messaging	• Message Waiting Indication
Centralized Attendant	• "Camp-on" on page 301 • "Break-in" on page 301

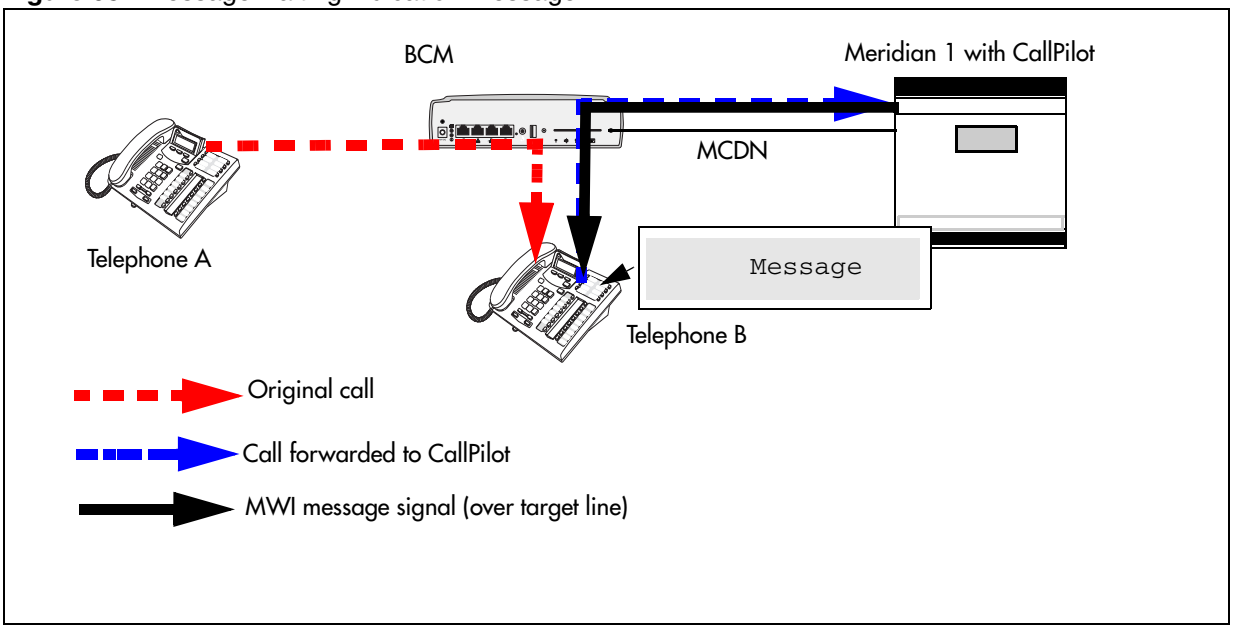
Message Waiting Indication

MWI allows the voice mail host system (Meridian 1) that is designated to receive messages to notify a target telephone on the BCM of a call waiting using the native MCDN MWI or MIK/MCK message indicators on the Meridian telephones. This feature works for both Nortel and third-party voice mail systems. Messages are received at a centralized location, to a predetermined telephone, where they are processed and forwarded to the target telephone.

MWI allows the user to reply or call back to the message center. The procedure for retrieving messages is described in the Telephone Features Handbook.

Figure 95 demonstrates how the Meridian responds when a call is forwarded to a CallPilot mailbox.

Figure 95 Message waiting indication message



Programming notes

BCM programming
To select Remote Capability for MWI on a per-loop basis for PRI: **Configuration > Resources > Telephony Resources > IP Trunks > H323 Settings**: Remote Capability MWI = select (if M1 has MWI package, with RCAP set to MWI)
Turning on the service for IP trunks: **Configuration > Resources > Telephony Resources > IP Trunks > H323 Settings**: Remote Capability MWI = select (if M1 has MWI package, with RCAP set to MWI)
Telset admin: Telco features, VMsg Ctr Tel Numbers: • Voice Message Center 1 set to destination code plus M1 voice mail DN
Lines (target line), Telco features: • **Configuration > Telephony > Lines > All Lines** > choose a target line to see the 'Voice message Center 1' feature under the 'Preferences' tab
Configuration > Telephony > Sets > Active sets > Line access > Line assignment: • assign target line to each set • in target line, select VMsg

M1 programming
1. Disable the PBX D-channel associated with IPT (LD96). 2. Add MWI to the RCAP of the D-channel (LD 17 RCAP MWI) 3. Ensure the RLS ID is a minimum of 25 (RLS ID 25). 4. Re-enabled the PBX D-channel. **Note**: Package 219 is required on the Meridian PBX to allow RCAP MWI. **Note**: If IP routing is being used, you must complete this procedure on all the D-channels in the private network.

Camp-on

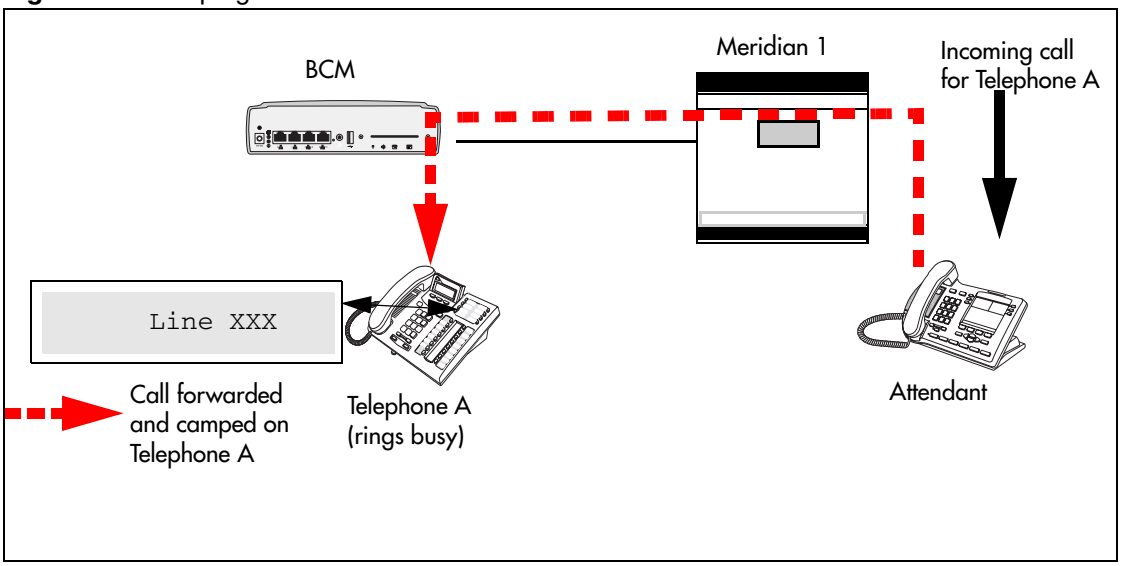
A call received by the Meridian attendant can be assigned to a telephone anywhere in the MCDN network, when the following situations are valid:

- the target telephone rings busy when the attendant calls
- no free keys on target telephone
- DND regular feature is inactive
- DND on busy feature is inactive

The target user sees that there is a call camped on the telephone. The called user can then clear a busy lines and take the call, or the user can choose to reject the call, using F814, or the user can indicate Do Not Disturb, using F85.

Figure 96 demonstrates the call path for a Meridian attendant to camp a call on a telephone in the system.

Figure 96 Camping a call

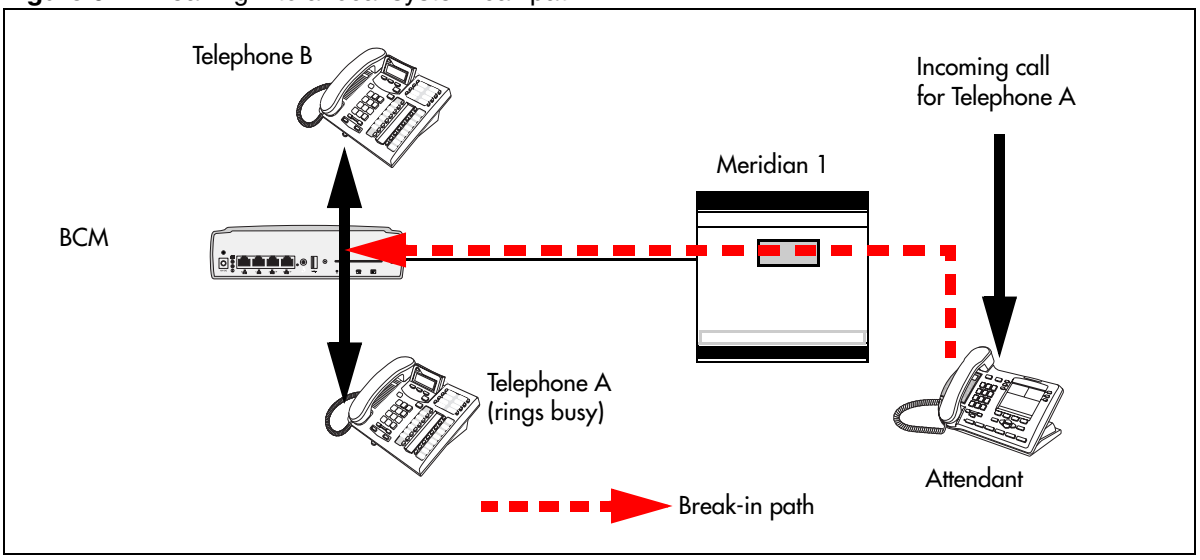


Break-in

The Meridian attendant can use the break-in feature to interrupt an ongoing call from a telephone in the system.

Figure 97 demonstrates the call path for a Meridian attendant to break into a call between telephones in the system.

Figure 97 Breaking into a local system call path



Break-in can occur when these situations are valid:

- Target system telephone is busy but still has a free intercom or line key.
- There is no camped call on the target telephone.
- DND on busy is turned on.
- prime set is also busy, with no free key, and with DND turned on.
- Attendant capability is high (2), and higher than either the target telephone or the caller the target telephone owner is busy with.

Only post-dial break-in is supported by MCDN:

1. Attendant dials destination number.
2. If a busy tone is heard, the attendant presses the BKI button.
   Attendant is given access to the conversation.

You can set a level of priority that will determine if a telephone will allow an attendant to break in. This is referred to as setting the Intrusion level. Use the following rules to configure the break-in feature.

- Set the Intrusion level for each telephone (under Capabilities on the DN record). Refer to "Capabilities tab" in the *Device Configuration Guide* (NN40020-300).

  How the intrusion hierarchy works:

  — Break-in is allowed if Attendant telephone is High and caller telephone is Medium.
  — Break-in is not allowed if Attendant telephone is Medium and caller telephone is high.

MCDN networking checklist

The following points provide a quick check for the system prerequisite settings for MCDN networking.

Select the dialing plan to be used:

- **UDP (Universal Dialing Plan)**
  - DNs on the same node are dialed directly.
  - DNs on other nodes are called by first dialing an Access Code and an ESN.
  - Each node has its own ESN.
- **CDP (Coordinated Dialing Plan)**
  - DNs on all nodes are dialed directly.

Ensure the following common programming is configured:

- **BCM Programming**
  - Configure the system DN length to match the DN length used in the rest of the private network.
  - Program the private Route: Type=Private, Dial=None.
  - Program the public Route: Type=Public, Dial=None.
  - Enable the MCDN Supplementary Services; TRO=selected, ICCL=selected, TAT=selected.
  - Program telephones with a target line that specifies the system DN of the telephone in the **Private received number** field.

Note: If you have public DNs set up for your telephones that are different from the system-assigned DN, each telephone needs to use the public and private received digits on the target line.

- **Meridian 1 Programming**
  - Program the system PNI and the PNIs for the routes.
  - Program the Meridian voice mailboxes (if required).
  - Enable the MCDN Supplementary Services: RCAP=[ND2,TRO,MWI], NASA=YES.

Set up the specific programming the system requires for the dialing plan. Refer to the following tables.

UDP-specific programming

BCM UDP programming		
• Private Dialing Plan:	Type=UDP, HomeLoc=<three-digit prefix>	
• Private Access Code	<unique code>	
• Private DN length	<total of Private Access Code + Location Code + DN length> Example: if dialing string is 6 393 2222, then set private DN to 8	
• Program the DestCodes for the other nodes	AccessCode plus the ESN, absorb the AccessCode. Example: For AccessCode=6; DestCode=6393[Absorb=1]	

M1 UDP programming		
• Private Access Code	Overlay 86, LD 86 REQ: PRT CUST: 0 FEAT: ESN	To change Private Access Code: Overlay 86, LD 86 REQ: CHG CUST: 0 FEAT: ESN, keep pressing until you reach the AC1 prompt At the AC1 prompt, make your choice
• Check UDP programming	Overlay 90, LD 90 REQ: PRT CUST: 0 FEAT: NET TYPE: LOC LOC: press enter, all the programmed location codes are listed HLOC is the home location of the M1	
• Program UDP values to route	Overlay 90, LD 90 REQ: CHG CUST: 0 FEAT: NET TYPE: AC1 LOC: (enter a number) RLI: (enter the RLI corresponding to the route)	

CDP-specific programming

BCM CDP programming		
• Private Dialing Plan: Private Access Code <unique code>.	Type=CDP	
• Private DN length	<system DN length>	
• PNI	<number assigned from M1 (1-127)>	
• Program the DestCodes for the other nodes	use Steering code as part of dial string	
M1 CDP programming		
• PNI	LD 16, RDB - PNI in M1 programming LD 15 - Net - PNI in M1 programming set to PNI of switch	
• Distant Steering Codes	Overlay 87, LD 87 REQ: PRT CUST: 0 FEAT: CDP TYPE: DSC (Distant Steering Code) DSC: press enter (lists all DSC programmed)	
• Check RLI (Route Line Index)	Overlay 86, LD 86 REQ: PRT CUST: 0 FEAT: RLB PLI: press enter (displays all the RLIs)	
• Program new CDP value to route	Overlay 87, LD 87 REQ: CHG CUST: 0 FEAT: CDP TYPE: DSP DSC: enter number (enter common BCM system number, for example if DNs are 4XX, enter 4) RLI: enter the RLI that corresponds to the route	

VM programming with Meridian 1

If you are using the centralized voice message system from a Meridian 1 system, you require the following programming on the M1:

M1 programming in LD 17

- NASA selected
- NCRD selected

<table>
<tr><td colspan="4">Verifying NASA is Active
• Overlay 22, LD 22
• REQ: PRT
• TYPE: ADAN DCH (slot number)
• NASA should be selected</td></tr>
<tr><td>If NASA is not on:</td><td>Disable the D channel
• Overlay 96, LD 96
• REQ: CHG
• TYPE:DISDCH</td><td>Disable the loop
• Overlay 60, LD 60
• REQ: CHG
• TYPE: DISL (slot number)</td><td>Program the D channel
• Overlay 17, LD 17
• REQ: CHG
• TYPE: ADAN
• ADAN: CHG DCH (slot number)
• Keep pressing enter until you get to NASA
• TYPE: yes
• TYPE: end</td></tr>
<tr><td colspan="2">Verifying NCRD
• Overlay 20, LD 20
• REQ: PRT
• TYPE: TIE
• CUST: 0
• Route: Enter the route defined in LD 20
• Keep pressing enter until all values are displayed. Check if NCRD is yes.</td><td colspan="2">If NCRD is set to no
• Overlay 16, LD 16
• REQ: CHG
• TYPE: RDB
• CUST: 0
• ROUT: (route number) from LD 20
• Keep pressing enter until you get NCRD and type Yes
• Keep pressing enter until you get the REQ prompt again
• TYPE: end</td></tr>
</table>

Meridian TRO programming

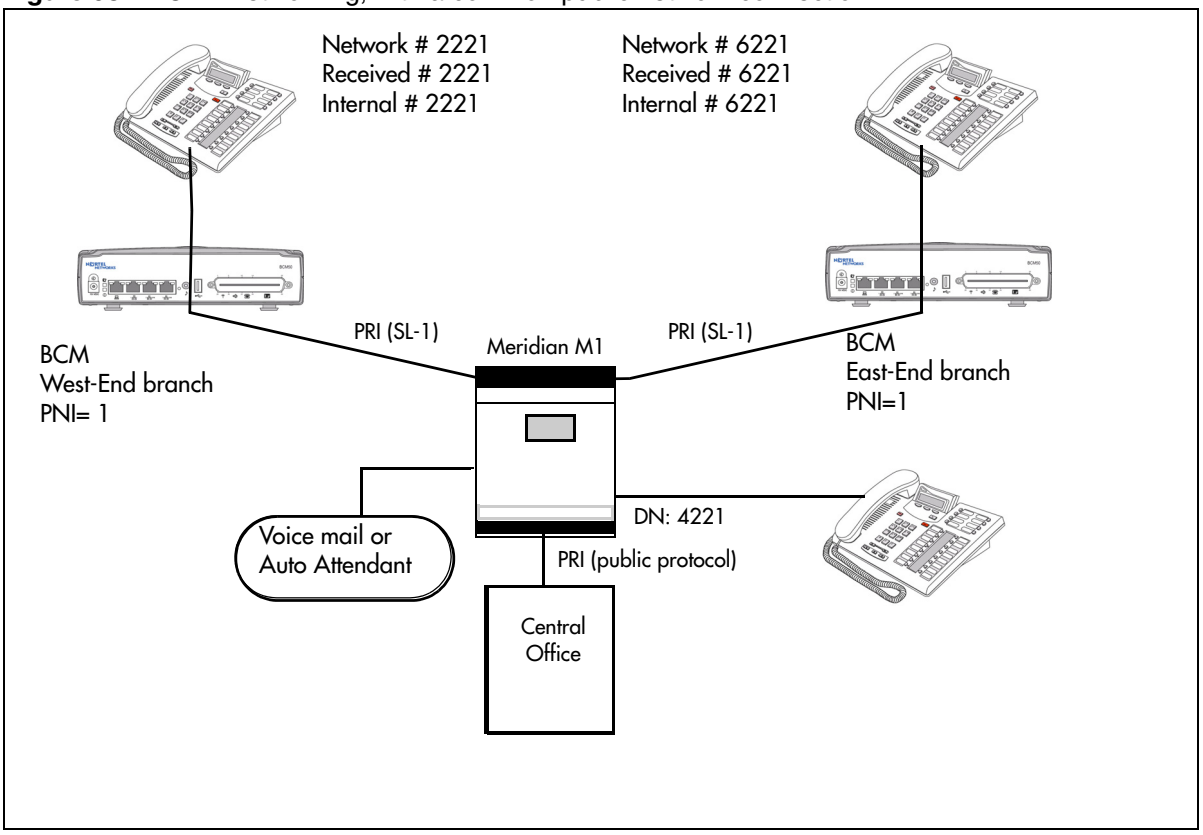
If you are using a Meridian 1 system as part of the network, you need the following programming for each system:

```
M1 TRO set to yes for BCM route:
LD 16
TYPE: RDB
Cust: xx
Rout: 0-511
TRO: Yes
```

An example of a private network with Meridian 1

Figure 98 shows a private network composed of one central Meridian 1, and two sites with BCM systems all connected by SL-1, with MCDN activated on all sites. This example uses a coordinated dialing plan (CDP). The DNs consist of four digits. The first digit is a destination code which is specific to each system. The last three digits are unique to each telephone within that system. Refer to "Dialing plan: Private network settings" on page 281 for a description of the dialing plans available to private networks.

Figure 98 MCDN networking, with a common public network connection



This example could represent a large head office (the Meridian 1) connected to several smaller branch offices (the two BCMs). In this network, only the head office has trunks connected to the public network.

The branch offices access the public network through the PRI to the head office. This configuration allows for cost savings by consolidating the public access trunks. Users at all three locations access the public network by dialing 9, followed by the public number. For example, a user in the West End branch might dial 9-555-1212 (for a local call) or 9-1-613-555-1212 (for a long-distance call). The BCM routing table routes these public calls to the Meridian 1. Routing tables at the Meridian 1 will then select an appropriate public facility for the call.

Note that the Private Network Identifier (PNI) is programmed at each end of the links. The PNI identifies the BCM to the Meridian 1 system.

Routing is set up such that network calls are made by dialing a four-digit private network DN. For example, if a user in the West End branch wishes to call a user in the East End branch within the private network, they dial 6221. Figure 98 illustrates this example.

The implications on the configuration on each node to access the PSTN through one network node:

- Each node must have the Private Network Access Code set to the value 9.
- Each node must have destination codes that match the Private Network Access Code plus digits corresponding to calls terminating in the local PSTN. For example, if the Private Network Access Code is 9, the node in Ottawa would require a destination code of 91613. Similarly, Toronto would require the following destination code: 91416.

BCM module settings: Table 60 lists the module settings that are required to set up the network described in Figure 98.

Table 60 Module settings for MCDN network

West End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary
East End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary

BCM dialing plan settings: Table 61 lists the dialing plan settings that are required to set up the network described in the figure in the previous section.

Table 61 MCDN dialing plan settings

West End office:		
Dialing Plan programming	Type	CDP
	Private Network ID	1
	Private DN Length	4
	Public DN Length	7
East End office:		
Dialing Plan programming	Type	CDP
	Private Network ID	1
	Private DN Length	4
	Public DN Length	7

BCM routing information: Table 62 lists the lines and routing information required to set up the network shown in Figure 98.

Table 62 Network routing information (Sheet 1 of 2)

West End office:			
Trunk/Line Data	Line 125	Target line	
	Private Received #	2221	
Line Access	DN 2221	L125:Ring only	
	Line pool access	Line pool BlocA	
Routing Services	Private Network		Public Network
	Head Office and East end		
Route	001		002
External #	No number		No number
Use	Pool BlocA		Pool BlocA
DN type	Private		Public
Destination codes for routes to:	Head office to M1	Head office to East End	
Destination Code	4 (includes location code)	6	9
Normal route	001	001	002
Absorb	0	0	0

Table 62 Network routing information (Sheet 2 of 2)

East End office:			
Trunk/Line Data	Line 125	Target line	
	Private Received #	6221	
Line Access	DN 6221	L125:Ring only	
	Line pool access	Line pool BlocA	
Routing Services	Private Network		Public Network
	Head Office to West End		
Route	001		002
Dial out #	No number		No number
Use	Pool BlocA		Pool BlocA
DN type	Private		Public
	Head Office to M1	Head Office to West End	Call terminates at M1
Destination Code	4 (contains location code)	2	9
Normal route	001	001	002
Absorb	0	0	0

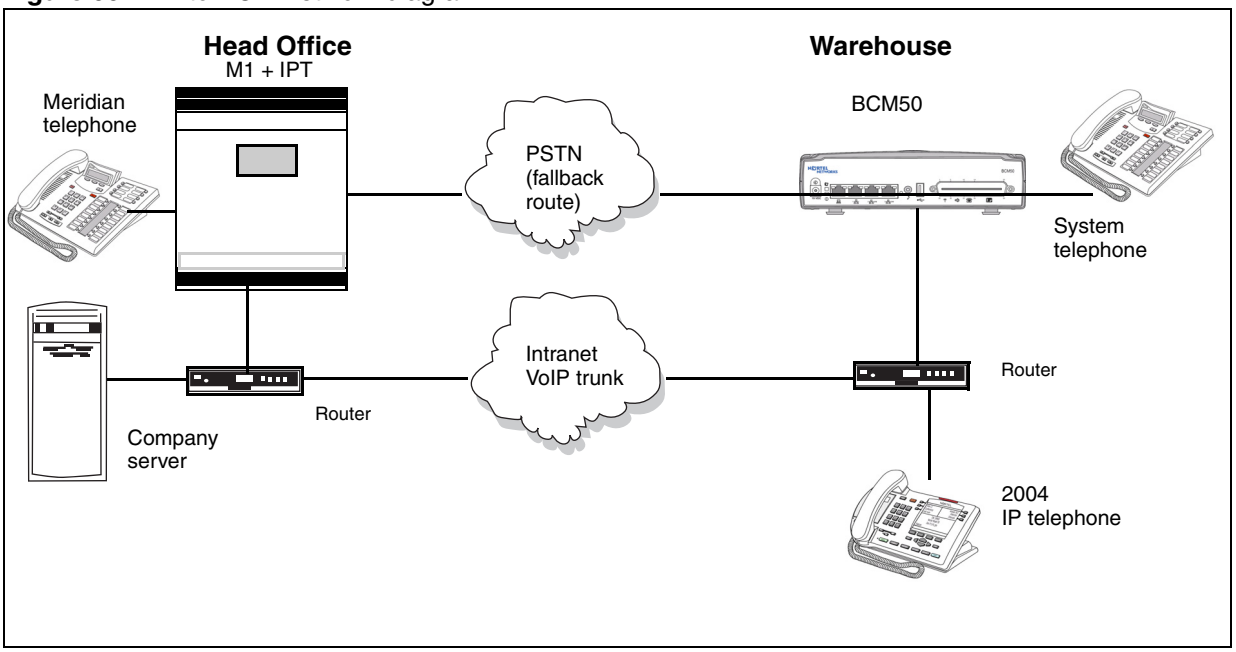
Configuring fallback over a VoIP MCDN network

The Voice over IP (VoIP) MCDN networking protocol between a Meridian 1 and one or more BCMs works the same way as it does over PRI lines. You still require the MCDN and IP telephony software keys and compatible dialing plans on all networked systems.

The one difference between MCDN over PRI and MCDN over VoIP is that the VoIP trunks require specific Remote Gateway settings, unless there is a Gatekeeper configured to route traffic on the IP network. You must also ensure that your PSTN fallback line is a PRI SL-1 line, to maintain MCDN features on the network.

Refer to Figure 99 for an example.

Figure 99 M1 to BCM network diagram



To set up the M1 in a BCM network

1 Make sure the M1 IPT meets the following requirement:

- IPT version 3.0 or newer

2 Ensure that the M1 ESN programming (CDP/UDP) is compatible. For information about this, refer to your M1 documentation.

3 On the BCM Element Manager:

- Set up outgoing call configuration for the VoIP gateway.
- Set up a remote gateway for the Meridian 1.
- Ensure the dialing rules (CDP or UDP) are compatible with the M1.
- Configure the PSTN fallback, and enable QoS on both systems.
- If target lines have not already been set up, configure the telephones to receive incoming calls through target lines.

MCDN functionality on fallback PRI lines

To enable MCDN functionality over PRI fallback lines

- Check MCDN PRI settings on the M1. For information on this, refer to the M1 documentation.
- Ensure SL-1 (MCDN) keycodes are entered on the BCM and the PRI line is set up for SL-1 protocol.

For a detailed description of setting up fallback, refer to "Setting up VoIP trunks for fallback" on page 391.

Networking with ETSI QSIG

(International systems only)

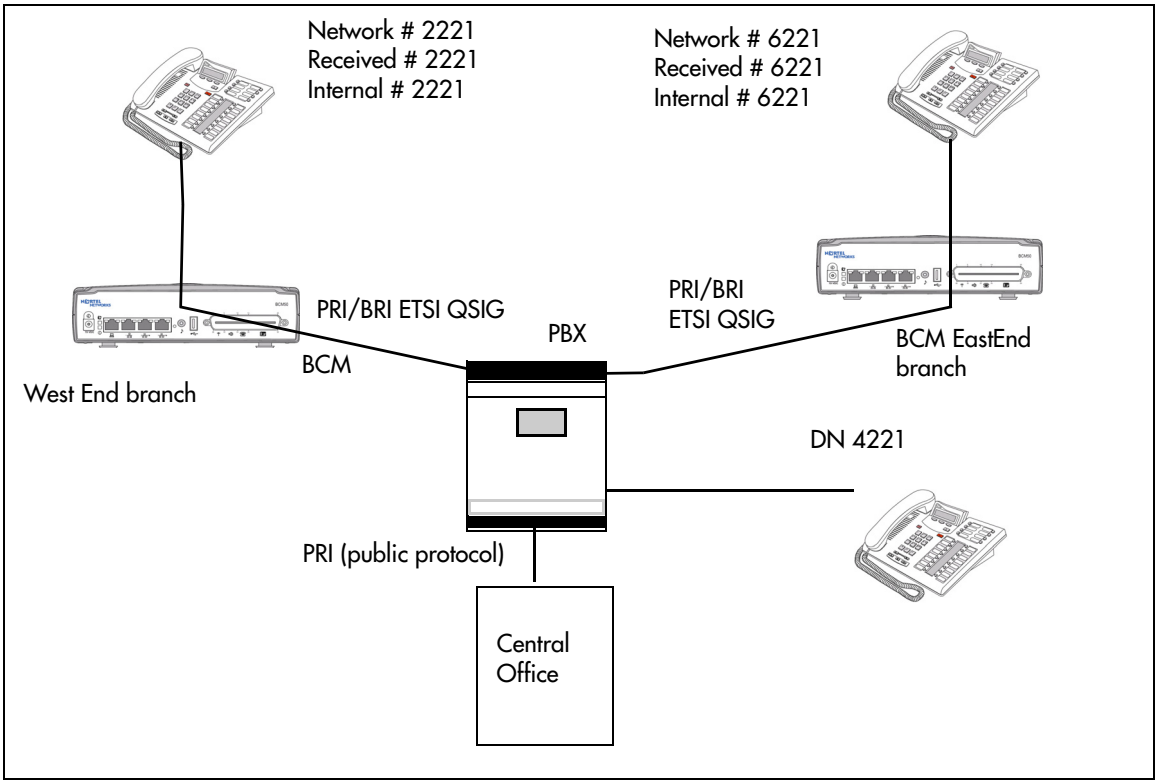
ETSI QSIG is the European standard signaling protocol for multi-vendor peer-to-peer communications between PBX systems and/or central offices.

Also refer to "Configuring ETSI Euro network services" on page 321.

Figure 100 illustrates an ETSI QSIG network. Note that this is exactly the same setup as that shown in the MCDN section for North America, in "An example of a private network with Meridian 1" on page 307, which describes PRI SL-1 networking. The exception in the configuration is for the hardware configuration because the trunk lines are different. The hardware programming for ETSI QSIG is described below the following diagram. All other configurations are the same as those shown in the MCDN section for North America, in "Using MCDN to network with a Meridian system" on page 297.

Note: Features for ETSI Q.sig are basic compared to MCDN. Only basic call and calling number is supported as opposed to the many MCDN features.

Figure 100 ETSI QSIG networking



Settings for some of the hardware parameters for the ETSI QSIG networking example shown above are as follows.

West End office:		
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

East End office:		
Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)
	ClockSrc	Primary

Chapter 33
Private networking: Basic parameters

The following provides an overview of the values in the system that affect private networking, including:

- "Private networking protocols" on page 315
- "Keycode requirements" on page 315
- "Remote access to the network" on page 316
- "Other programming that affects private networking" on page 316
- "Types of private networks" on page 316

Private networking protocols

The BCM supports the following protocols for private networking:

- PRI: ETSI QSIG, MCDN, DPNSS
- BRI: ETSI QSIG
- T1: E&M
- VoIP: MCDN

BCM systems can be networked together using TIE lines or E&M connections. Larger networks, or networks that are geographically spread out, can be chained together through faster PRI SL-1 connections or with voice over IP (VoIP) trunk lines. SL-1 lines and VoIP trunks also offer the opportunity to use the MCDN protocol, which provides enhanced trunking features and end-to-end user identification. If a Meridian 1 is part of the MCDN network, the network can also provide centralized voice mail and auto attendant off the Meridian.

MCDN note: MCDN networking requires all nodes on the network to use a common Universal Dialing plan (UDP) or a Coordinated Dialing Plan (CDP). Refer to "Dialing plan: Public network," on page 275 and "Dialing plan: Private network settings," on page 281.

Keycode requirements

Keycodes are required to activate the protocols that are used to create private networking, including:

- IP trunks, if you want additional IP trunks
- an MCDN keycode, if you want to use the MCDN protocol between the systems

You must purchase and install these keycodes before you can create any of the networks described in this chapter. Consult with your Nortel distributor to ensure you order the correct keycodes for the type of network you want to create.

Remote access to the network

Authorized users can access TIE lines, central office lines, and BCM features from outside the system. Remote users accessing a private network configured over a large geographical area, can potentially also place long-distance calls through the network and avoid toll charges. Also refer to "Call security and remote access" on page 415.

Note: You cannot program a Private DISA DN or Private Auto DN to a VoIP trunk, as they act as auto-answer trunks from one private network to the next. However, you can configure VoIP line pools with remote access packages so that callers can access telephones or the local PSTN on remote nodes on a tandemed network that use VoIP trunks between systems.

Other programming that affects private networking

Besides the line programming, these links connect to other programming that affects or is affected by private networks.

- "Dialing plan: System settings," on page 267 (Received Number Length)
- "Module configuration: Trunk modules" on page 81
- "Configuring lines" on page 129
- "Configuring lines: Target lines," on page 141
- "Dialing plan: System settings," on page 267
- "Dialing plan: Routing and destination codes," on page 259
- "Call security: Restriction filters," on page 433
- "Call security: Remote access packages," on page 439
- "Configuring CLID on your system," on page 205
- "Line Access tab" in the *Device Configuration Guide* (NN40020-300) (Private OLI)

Types of private networks

There are several ways you can create private networks. Configuration can be based on such things as cost of trunks, proximity of network nodes, size of the private network, and business requirements for communications.

VoIP-based networking also requires an understanding of IP features such as codecs, jitter buffers, Quality of Service (QoS) function, and silence suppression.

The services provided within networks is based on the type of trunks and the protocols assigned to the trunks. All trunks within the network should be running the same protocols, to provide a consistent look and feel to the users.

These are the main types of private networking, listed from the simplest to the more complex PRI/ETSI and VoIP routing using MCDN protocols:

- "Private networking: Using destination codes," on page 339
- "Private networking: PRI Call-by-Call services," on page 343
- "Private networking: PRI and VoIP tandem networks," on page 323
- "Private networking: MCDN over PRI and VoIP," on page 297
- "Private networking: DPNSS network services (UK only)," on page 331

Chapter 34
Private networking: MCDN and ETSI network features

If the MCDN protocol is added to a PRI SL-1 or VoIP private network, the network provides additional network-management features and provides available centralized voice mail features to all nodes on the network.

ETSI lines (UK profile) also have network features available from the central office that can be enabled or disabled.

The following describes the different aspects of SL-1 and MCDN private networking.

- "Configuring MCDN network features" on page 319
- "Configuring ETSI Euro network services" on page 321

Configuring MCDN network features

When you connect your BCM systems through PRI SL-1 or VoIP trunks and activate the MCDN protocol, your network provides a number of network call features. You can use this protocol to network other BCM systems, Norstar systems, Meridian 1 systems, Succession systems, and DMS-100 systems.

Table 63 lists the MCDN features that are provided by all SL-1/VoIP networks where MCDN is active. The features affect call redirection and trunking functions.

Table 63 MCDN network features

Centralized messaging	"Configuring Network Call Redirection Information" on page 319 (NCRI)
Centralize trunking	"ISDN Call Connection Limitation" on page 320 (ICCL) "Trunk Route Optimization (TRO)" on page 320 (TRO) "Trunk Anti-tromboning (TAT)" on page 320 (TAT)

Configuring Network Call Redirection Information

NCRI provides call information in the network when calls are redirected from one system to another. NCRI builds on the following BCM features:

- External Call Forward
- Call Transfer
- Call Forward

ISDN Call Connection Limitation

The ICCL feature piggybacks on the call initiation request and acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.

To configure ICCL

1. Click **Configuration > Telephony > Dialing Plan > Private Network**.
2. Locate the Private Network/MCDN subpanel.
3. Select the **Network ICCL** check box.
4. Click **Configuration > Resources > Telephony Resources**.
5. From the Modules table, select the required module.
6. Locate the Details for Module subpanel.
7. Click the Trunk Module Parameters tab.
8. Enter the Maximum transits in the Maximum transits field.

Trunk Route Optimization (TRO)

TRO finds the most direct route through the network to send a call between nodes. This function occurs during the initial alerting phase of a call.

To enable TRO

1. Click **Configuration > Telephony > Dialing Plan**.
2. Locate the MCDN subpanel.
3. Select the **TRO** check box.

Trunk Anti-tromboning (TAT)

TAT is a call-reroute feature that works to find better routes during a transfer of an active call. This feature acts to prevent unnecessary tandeming and tromboning of trunks.

Note: TAT is not applicable for alerting calls.

To enable TAT

1. Click **Configuration > Telephony > Dialing Plan > Private Network.**
2. Locate the MCDN subpanel.

3 Select the **TAT** check box.

Configuring ETSI Euro network services

If your system has ETSI ISDN BRI/PRI lines, you can activate the malicious call identification (MCID) and Network Diversion features. Advice of Charge-End of Call (AOCE) is active if your service provider has activated that service on the line.

When the features are activated, users can:

- display a call charge
- redirect calls over the ETSI ISDN BRI/PRI line to the outside network
- tag malicious calls

Advice of Charge-End of Call (AOCE) — AOCE is a supplementary service available from your service provider on ETSI ISDN BRI/PRI links. With this feature, the BCM user can view the charges for an outgoing call once the call completes. This information is also reported to the Call Detail Reporting Application. The information can be provided in currency or charging units, depending on how the feature is set up by your service provider.

To invoke the feature, the user presses **FEATURE 818**.

To enable MCID and network diversion

1 Click **Configuration > Telephony > Dialing Plan > Private Network**.

2 Locate the ETSI subpanel.

Select the check boxes of the required options.

Table 64 lists the possible values for ETSI.
The **Description** column of the table describes the feature and how the user activates each feature from their telephone.

Table 64 ETSI network values

Attribute	Values	Description
Netwrk Diversion	<check box>	Allows calls to be redirected to an outside network.
MCID	<check box>	Malicious Call Identification When selected, the called party can use **FEATURE 897** to request the network to record the identity of an incoming call. including: • called party number • calling party number • local time and date of the activity • calling party sub-address, if provided by the calling user
MCID note		The feature code must be entered within 25 seconds of the caller hanging up. (A 25-second busy tone occurs.) If the called party hangs up first, there is no opportunity to use the feature. **Note**: The call identification comes from your service provider, not the BCM. You must have the service activated by the CO before the feature is active for the user, regardless of the setting in this field.

Chapter 35
Private networking: PRI and VoIP tandem networks

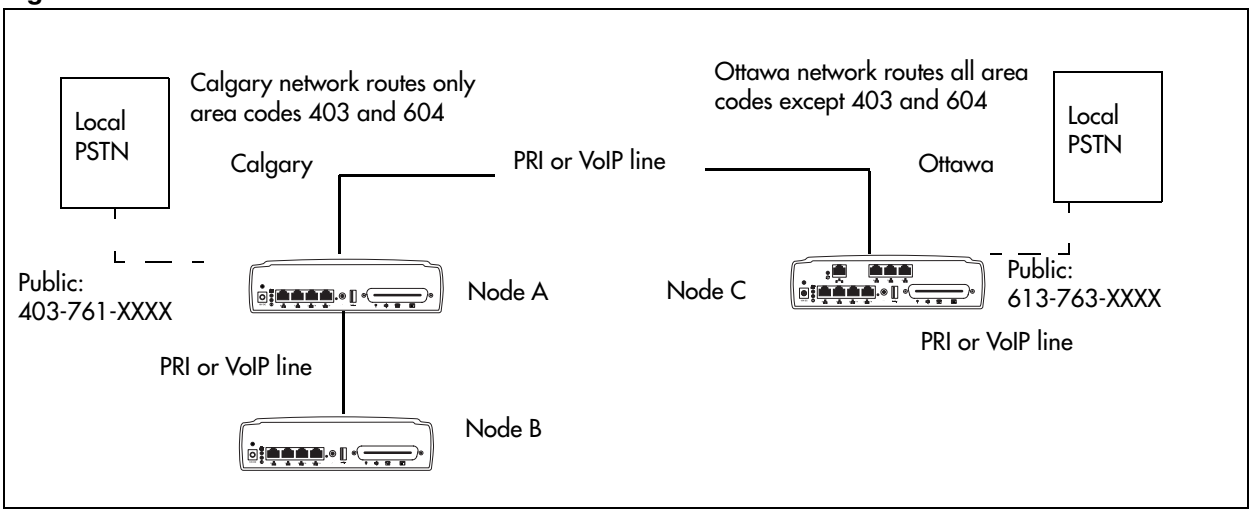
You can use PRI trunks and VoIP trunks to create a private network between other BCMs. This tandem network provides you with the benefits of end-to-end name display and toll-free calling over the PRI or VoIP private link. Each BCM becomes a node in the network.

Refer to the following information about tandem networks:

- "Routing for tandem networks" on page 323
- "Routing calls through a tandem network" on page 324
- "Using VoIP to tandem systems" on page 327

Figure 101 demonstrates a tandem configuration.

Figure 101 Private tandem network of BCMs



Also refer to "Using VoIP to tandem systems" on page 327 for other examples of tandem systems using VoIP trunks.

Routing for tandem networks

In this type of network, each Business system node is set up to route calls internally as well as to other nodes on the system. Each node must have a unique identification number, which is determined by the type of dialing plan chosen for the network.

VoIP trunks require local gateway configuration and either remote gateway or Gatekeeper configurations that identify the other nodes in the network.

If the node is also connected to the public network, the usual routing is required for that connection.

The following tables show the routing tables for Node A and Node C for external and internal terminating calls.

Table 65 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	91604
3 (Node B)	0	91403762 (Node B)
4 (PSTN)	1	9140376* (not internal network)
4 (PSTN)	1	914037* (not internal network)
4 (PSTN)	1	91403* (not internal network)
4 (PSTN)	1	9* (not internal network)
* This wild card represents a single digit.		

Table 66 Node A destination code table, internal termination

Route	Absorb length	Destination code (private DNs)
3 (Node B)	0	392 (Node B)
5 (Node C)	0	393 (Node C)

Table 67 Node C destination code table, external termination

Route	Absorb length	Destination code (Public DNs)
3 (Node B)	0	91613764 (Node D)
3 (Node B)	0	91613766 (Node F)
4 (PSTN)	1	9161376* (not internal network)
4 (PSTN)	1	916137* (not internal network)
4 (PSTN)	1	91613* (not internal network)
4 (PSTN)	1	9161* (not internal network)
4 (PSTN)	1	916* (not internal network)
4 (PSTN)	1	91* (not internal network)
4 (PSTN)	1	9 (not internal network)

Table 68 Node C destination code table, internal termination

Route	Absorb length	Destination code (Private DNs)
5 (Node A)	0	391 (Node A)
5 (Node A)	0	392 (Node B)

Routing calls through a tandem network

The following provides a step-by-step description of how calls network through a tandem network:

- "Calls originating from the public network" on page 325
- "Calls originating in the private network" on page 326

Calls originating from the public network

Table 69 describes how each node handles calls originating from the public network into the system.

Table 69 Call originating from the public network to a tandem network (Sheet 1 of 2)

Received	Destination	Description
Node A	Node A	User in Calgary dials 761-xxxx number Incoming interface: Public DN type: Public Node A receives the call and identifies it as terminating locally. Uses target line to route call (Public received #). Destination: Local (target line)
Node A	Node B	User in Calgary dials a 762-xxxx number DN type: Public Node A receives it and identifies it as being for node B. Uses private trunk to route it to B. Incoming interface: Public Destination: Remote Node Outgoing interface: Private Node B receives the call and identifies it as terminating locally. Uses target line to route call (Private received #). Incoming interface: Private Destination: Local (target line)
Node A	Node C	An external user in Calgary dials a 761-xxxx number which is answered with DISA. Incoming interface: Public DN type: Public Destination: Local (DISA DN) User enters a CoS password and a private DN for Node C 6 + 393-xxxx DN type: Private Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: (DISA user) Destination: Remote node Node C receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)

Table 69 Call originating from the public network to a tandem network (Sheet 2 of 2)

Received	Destination	Description
Node A	Ottawa PSTN	An external user in Calgary dials a 761-xxxx number which is answered with DISA. User enters a CoS password and an Ottawa public network number. Incoming interface: Public DN type: Public Destination: Local (DISA DN) Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: Local (DISA user) Destination: Remote PSTN Node C receives the call and identifies it as a public number and routes it out over the local PSTN. Incoming interface: Private Destination: Local PSTN

Calls originating in the private network

Table 70 describes how each node handles calls originating in the public network.

Table 70 Calls originating from the private network within a tandem network (Sheet 1 of 2)

Received	Destination	Description
Node B	Node B	DN is internal, therefore no trunk routing is required. Incoming interface: Intercom DN type: Local Destination: Local
Node A	Ottawa PSTN	User in Node A dials the private network access code for Node C, followed by an Ottawa public number. Incoming interface: Intercom DN type: public Destination: Remote PSTN Node C receives the call and identifies it as being for the public network. Node C routes the call over the local public network. Incoming interface: Private DN type: Public Destination: Local PSTN
Node B	Calgary PSTN	User on Node B dials a public DN. Node B recognizes it as being the responsibility of Node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node Node A receives the call and identifies it as being for the public network. Node A routes the call over the local public network. Incoming interface: Private Destination: Remote PSTN

Table 70 Calls originating from the private network within a tandem network (Continued) (Sheet 2 of 2)

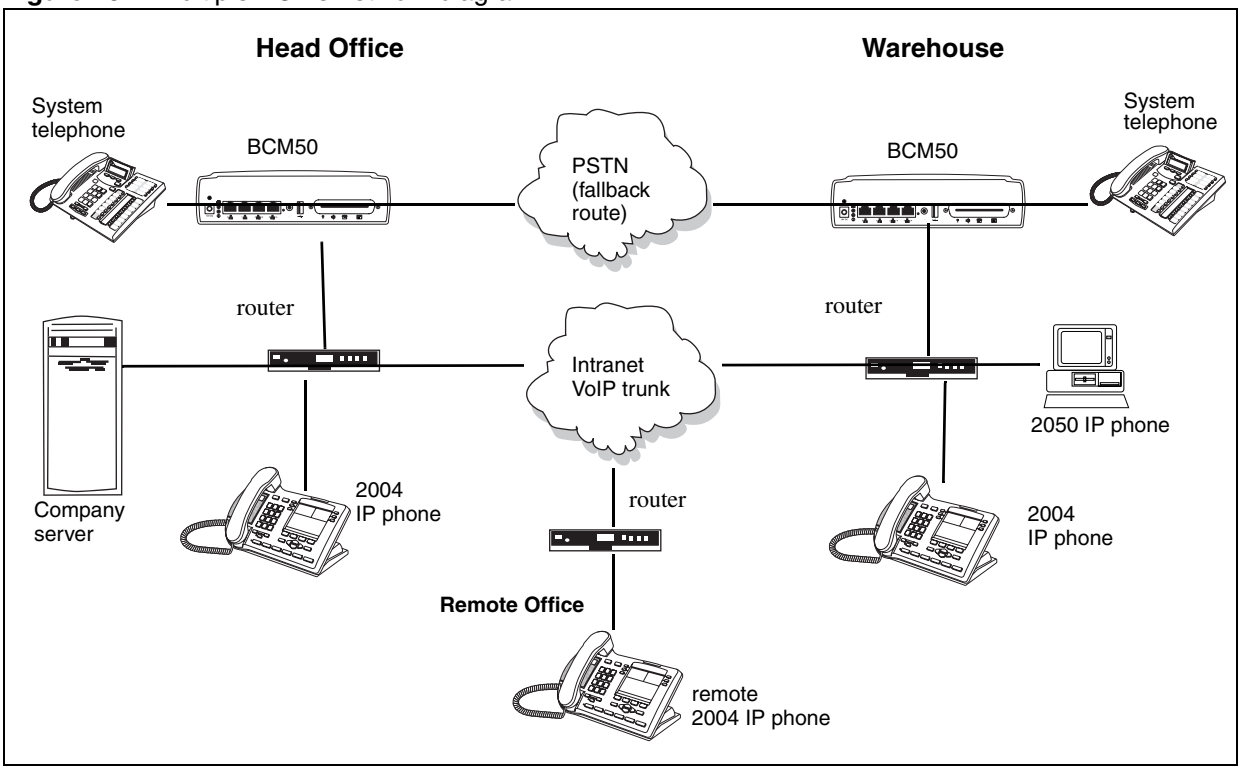
Received	Destination	Description
Node B	Node A	User in Node B dials a private DN for a user on A. DN type: Private Node B recognizes it as being for Node A. Uses the private trunk to route the call the call to A. Incoming interface: Intercom Destination: Remote node Node B receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)
Node B	Node C	User on Node B dials a private DN for a user on C. DN type: Private Node B recognizes it as being the responsibility of Node A and routes the call over the private trunk to A. Incoming interface: Intercom Destination: Remote node Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Private Destination: Remote node Node C receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)

Using VoIP to tandem systems

You can connect multiple offices with BCMs across your company intranet. With this installation CallPilot directs calls throughout the system or for one system to support voice mail for the network. Full toll bypass occurs through the tandem setup, meaning that any user can call any DN without long distance charges being applied. Users have full access to system users, PSTN connections.

Figure 102 demonstrates a multiple-BCM50 network. The network diagram shows two BCMs, but additional base units can be added.

Figure 102 Multiple BCMs network diagram



To set up a network of BCMs

1 Ensure that the existing network can support the additional VoIP traffic.

2 Coordinate a Private dialing plan between all the systems.

3 On each BCM:

- Set up outgoing call configuration for the VoIP gateway.
- Set telephones to receive incoming calls through target lines.
- Configure the PSTN fallback and enable QoS on both systems.

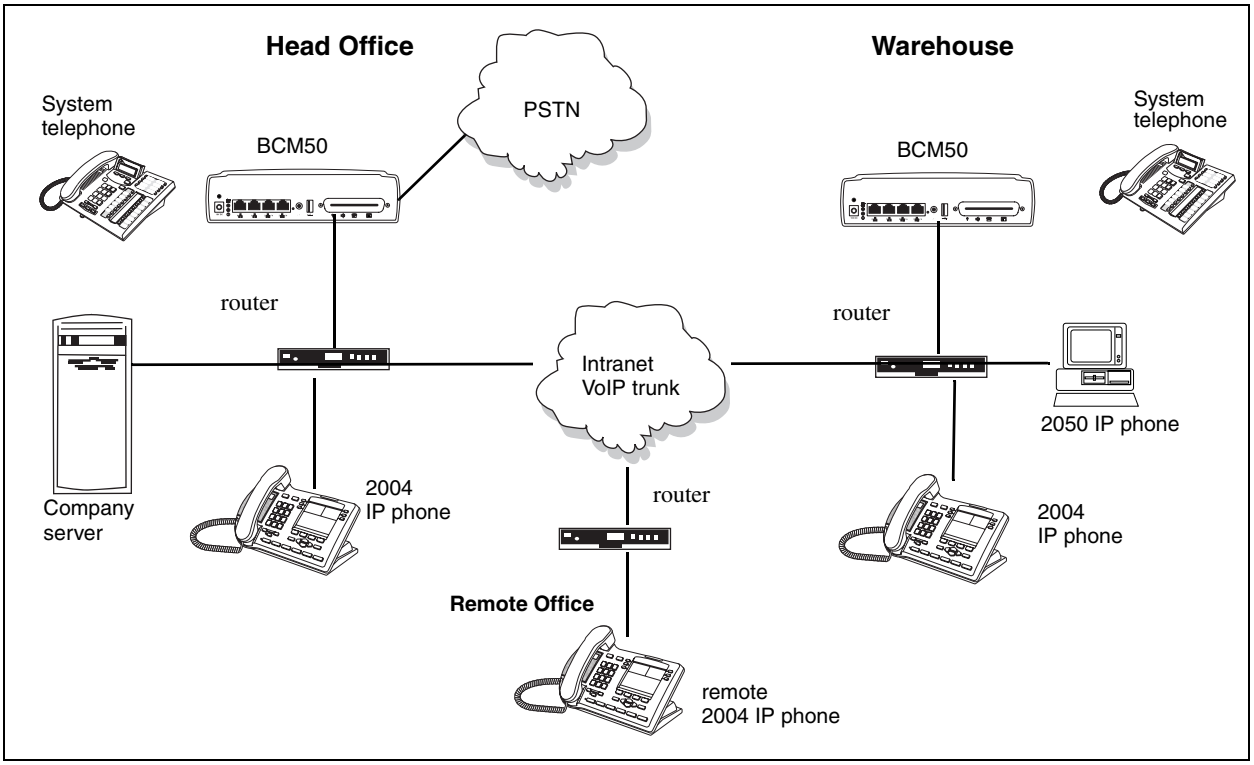
This system uses fallback to PSTN so calls can be routed across the PSTN connection if VoIP traffic between the BCMs becomes too heavy.

If only one of the BCMs in a network has a line to the PSTN network, all public calls from other systems are funneled through the system with the PSTN connection, and all communication between the systems occurs over VoIP trunks. To facilitate this system, you need to ensure that the destination codes on the non-PSTN system point to the system connected to the PSTN, and then, to the PSTN. On the PSTN-connected system, the system and destination codes must be configured to recognize and pass public calls from the other system out into the PSTN network. Since the receiving PSTN sees the calls as remote dial-ins, ensure that the correct remote access packages have been established for the VoIP trunks.

This also means that if the VoIP trunks are inaccessible between the systems, there is no provision for a fallback route.

Figure 103 demonstrates an example of routing all public calls through one BCM50.

Figure 103 Routing all public calls through one BCM



Chapter 36
Private networking: DPNSS network services (UK only)

Programming note: software keys are required to enable DPNSS 1. DPNSS 1 is not available on all profiles.

The following features are available and can be programmed over DPNSS lines:

- Diversion ("Using the diversion feature" on page 331)
- Redirection ("Using the Redirection feature" on page 333)
- "Executive intrusion, Intrusion protection level" on page 333
- "Call offer" on page 334
- "Route Optimization" on page 335
- "Loop avoidance" on page 335
- MWI is discussed with central voice mail setup ("Configuring centralized voice mail" on page 351)

Using the diversion feature

Diversion is a DPNSS 1 feature for BCM that allows users to forward their calls to a third party on the DPNSS 1 network. This feature is similar to call forward on BCM, but takes advantage of the broader capabilities of DPNSS.

There are five variations of Diversion: Call Diversion Immediate, Call Diversion On Busy, Call Diversion On No Reply, Bypass Call Diversion, and Follow-me Diversion. These variations are described below:

- Diversion Immediate diverts all calls to an alternate telephone. This function is programmed by the user at their telephone.
- Diversion On Busy diverts all calls to an alternate telephone when a telephone is busy. This feature is programmed in the Element Manager.
- Diversion On No Reply diverts calls that go unanswered after a specified amount of time. This feature is programmed in the Element Manager.
- Bypass Call Diversion overrides all call forward features active on a telephone over a DPNSS line. An incoming call to the telephone will not be forwarded; instead, the telephone will continue to ring as if call forward were not active. This feature is used to force a call to be answered at that location. Bypass Call Diversion is a receive-only feature on BCM, and cannot be used from a BCM telephone.

- Follow-me Diversion is also a receive-only feature. It allows the call forwarded destination to remotely change the BCM call-forwarding programming (Call Forward All Calls (CFAC) feature) to a different telephone.

Note: BCM CFAC must be active, and the destination set/PBX system must support the feature.

For example, user A forwards all calls to telephone B, a temporary office. Later, user A moves on to location C. The user does not have to be at telephone A to forward calls to location C. Using telephone B and Follow-me Diversion, the user can forward calls from A to location C.

Follow-me diversion can be cancelled from the forwarded location.

- Diversion on Busy and Diversion on No Reply cannot be cancelled from the forwarded telephone. These are programmable only by an installer and not by the user.
- If multiple telephones are programmed to take a call, the first telephone to respond will act. All other telephones responding are ignored. Therefore, if the first telephone to respond has Diversion enabled, this feature will be invoked.

Restrictions by telephone type

- all variations supported on BCM digital and IP telephones
- ATA2/ASM8+—all variations supported on an ATA
- ISDN—all variations supported on ISDN telephones, except Diversion on Busy and CFWD Busy

Setting Diversion

You set Diversion for DPNSS in the same way as call forward. You will need to enter the end DN when prompted. You may also need to include the DPNSS 1 routing number.

DPNSS to Embark connections

DPNSS lines connected to an Embark switch perform call redirection/diversion using the Call Forward feature to create a tandem link back to the switch. Since this is different from other switches, you must select the type of switch DPNSS will be connecting to when you do module programming. Refer to “Configuring the trunk module parameters” on page 83.

Before you program Call Forwarding ensure that:

- Both real channels and virtual channels are provisioned.
- Destination or line pool codes are programmed for the DPNSS to Embark link.

Also, during programming for Call Forward No Answer and Call Forward on Busy, when you enter the **Forward to:** digits, the system does a validation check with the switch on the number. (**Configuration > Telephony > Sets, All DNs** panel, Line Access tab, and then double-click the required field to enter the DN).

Using the Redirection feature

Redirection is a DPNSS 1 feature similar to BCM Transfer Callback. With Redirection, the originating party can redirect a call awaiting connection, or re-connection, to an alternate destination after a time-out period. Failed calls can also be redirected. Priority calls are not redirected.

Diversion on No Reply feature takes precedence over Redirection.

Restrictions by telephone type

- For telephones with single line displays, the **#** key acts as MORE and the ***** key acts as VIEW
- ATA2/ASM8+—not supported
- ISDN—all variations supported on ISDN telephones

Setting redirection

The timer used for the network Callback feature is also used for redirection.

Executive intrusion, Intrusion protection level

Executive Intrusion (EI) is a DPNSS 1 feature that allows an operator, or other calling party, to intrude on a line when it is busy. An example of the use of this feature is to make an important announcement when the recipient is on another call.

EI is implemented on the BCM using Intrusion protection level (IPL). IPL has four settings, from None to High. A telephone set has the ability to break-in when the other telephone set has a lower IPL. The default setting is None and a setting of High prevents intrusion.

Restrictions by telephone type

- ATA2/ASM8+—supported
- ISDN—not supported

Programming IPL on a telephone

To program IPL

1. Click **Configuration > Telephony > Sets**.
2. On the panel, locate and click the Capabilities and Preferences tab.
3. Select the DN of the telephone set being programmed.
   The Details subpanel for that DN appears in the lower portion of the panel.
4. Click the Capabilities tab.
5. Locate the Intrusion protection level and select the required option from the drop-down menu.

Call offer

Call Offer over DPNSS 1 allows a calling party to indicate to the wanted party that there is an incoming call available, even though there is no answer button available to present the call on the telephone.

Restrictions by telephone type

- model 7000 telephone — associated LED or LCD flashes, and a tone is heard
- ATA2/ASM8+—Call Offer is supported as a Camp On feature, and a tone is heard
- ISDN—not supported

Note the following general conditions and restrictions:

- DND on busy must be programmed as N (**DN ##/Capabilities**) for a telephone to accept Call Offer.
- If CF on busy is programmed for the telephone, Call Offer is not accepted.
- The target line for the telephone must be set to: If **busy: busy tone**, which is the default. Refer to "Configuring lines: Target lines" on page 141.
- Call Offer does not work if sent over Manual answer lines. It is recommended that the lines be left at the default: **Auto**.

Note: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

Route Optimization

Route Optimization is a DPNSS 1 feature for BCM that allows calls to follow the optimum route between two end PBXs. This allows efficient use of network resources.

No system programming is required for the feature when BCM is working as a terminating PBX system. However, BCM must have a private access code programmed that maps to a valid destination code or line pool code on DPNSS lines. Further, Allow redirect must be set to selected. For more information, see Capabilities tab" in the *Device Configuration Guide* (NN40020-300).

Loop avoidance

To set Loop avoidance during hardware configuration

1. Click the keys beside **Configuration > Resources> Telephony Resources.**
2. In one of the expansion modules select **DPNSS**.
3. Click the **Trunk Module Parameters** tab.
4. Type a value (0-25) in the Maximum transits box.
   The default value is 25.

Private networking with DPNSS

(International only)

DPNSS supports the Universal Dialing Plan (UDP), an international standard for sending and receiving private numbers over networks. The UDP requires that a dialing number includes the following:

- a Private Access Code, programmed into the system as part of the destination code table to prevent conflicts with the internal numbering system. (**Configuration > Telephony > Dialing Plan > Private Network > Private Access Code**)
- a Home Location Code (HLC) assigned to each PBX system, and configured as part of the destination code (a maximum of seven digits). For each HLC, a destination code must be programmed in the system. (**Configuration > Telephony > Dialing Plan > Private Network > Location code**)
- a Directory Number (DNs) assigned to each extension as a line appearance. The DN appears as the last string segment in a dialed number. In the number 244-1111, 1111 is the DN.

A typical Private Number, using a private access code and dialed from another site on the network, appears below.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+ 848	+ 2222	= 6-848-2222

In this networking example, a private network is formed when several systems are connected through a Meridian M1 and a terminating BCM system. Each site has its own HLC and a range of DNs. Figure 104 illustrates this example.

Calls are dialed and identified to the system as follows:

- To reach a telephone inside the Private Network, at the BCM site, the user dials the DN of choice.
- To reach a telephone inside the Private Network, from another site, the user dials HLC + DN.
- To reach a telephone outside the Private Network, the user dials an Access Code + HLC + DN

  Each node has its own destination (dest) codes which includes the appropriate access and HLC codes to route the call appropriately.

Table 71 shows examples of the construction of numbers used when dialing within the example network. Note that 6 is the Private Access code.

Table 71 Calling numbers required for DPNSS network example

Calling Site	LOC/HLC	Calling Party Number	Called Site	Dialing String	Called Party Number
Site A	244	244 1111	Site B	6 668 2222	668 2222
Site B	668	668 2222	Site D	6 848 2222	848 2222
Site D	848	2222	Site D	2229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Figure 104 DPNSS networking

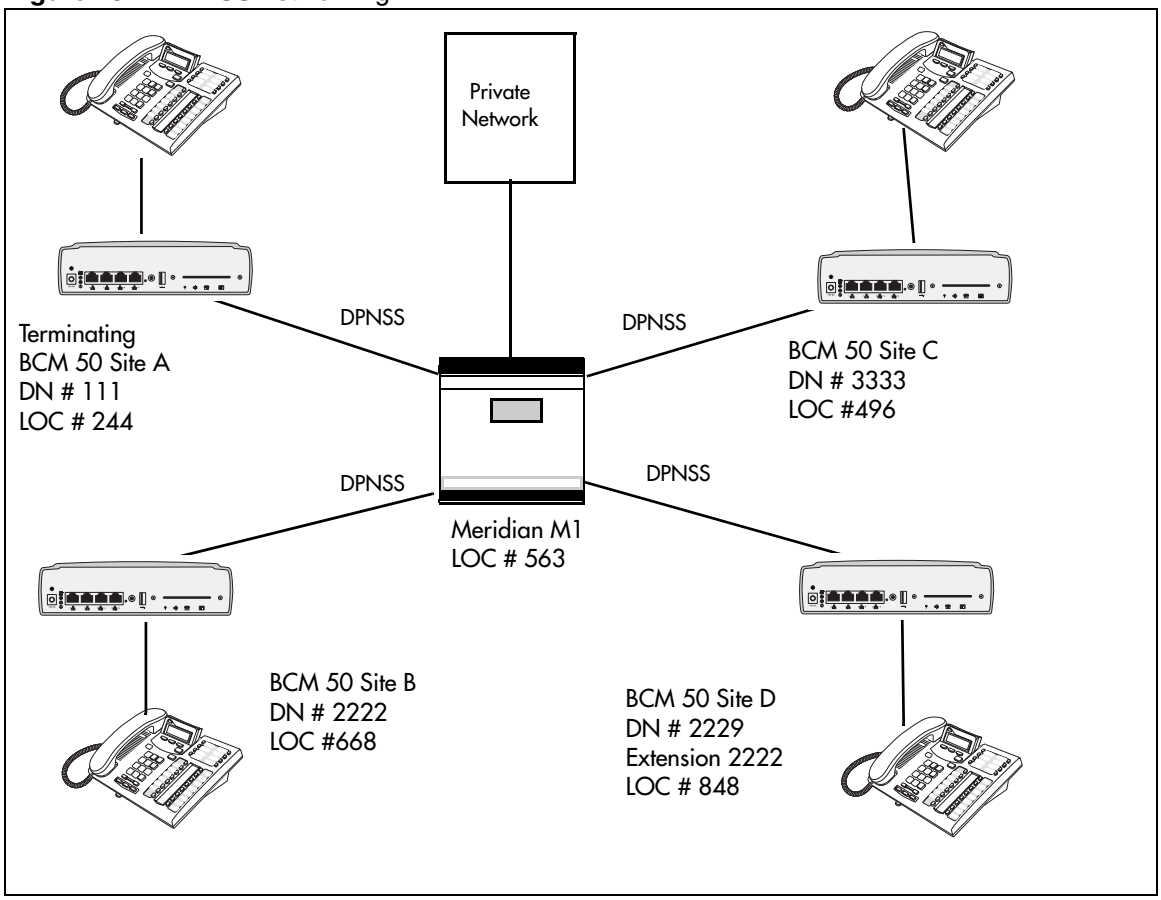


Table 105 shows examples of the routing required to set up the network shown in Figure 104. Note that 6 is the Private Access code.

Figure 105 Routing for DPNSS network

Private Network: (for each branch BCM)			
Routing service to		Private network	Public network
	Route	001	002
	Dial out #	No number	No number
	Use	Pool N	Pool N
	DN type	none (private access code 6 is programmed)	public
	Destination Code	6	9
	Normal route	001	002
	Absorb	1	1

Guidelines for creating a private dialing plan with DPNSS

Use the following guidelines when creating a private dialing plan with DPNSS.

- When creating HLCs for the nodes in your system, avoid numbering conflicts between network nodes and internal DNs, Hunt group DNs.
- Program a Private Access Code into your destination routing tables to avoid conflicts with your internal HLC and dest code dialing plan. For example, if a dialout HLC is 848, but this number already exists in the BCM system for an extension, the routing tables should add a Private Access Code to the dest code. If the code is programmed as 6, the dest code becomes 6848. 6848 uses a route to dial out 848 using the DPNSS line pool, allowing the call to be placed.

  Note that a Private Access Code is required only for specific DPNSS features such as Diversion, Route Optimization, and Redirection.

Customizing the DPNSS routing service

You can customize the routing service using the following restrictions:

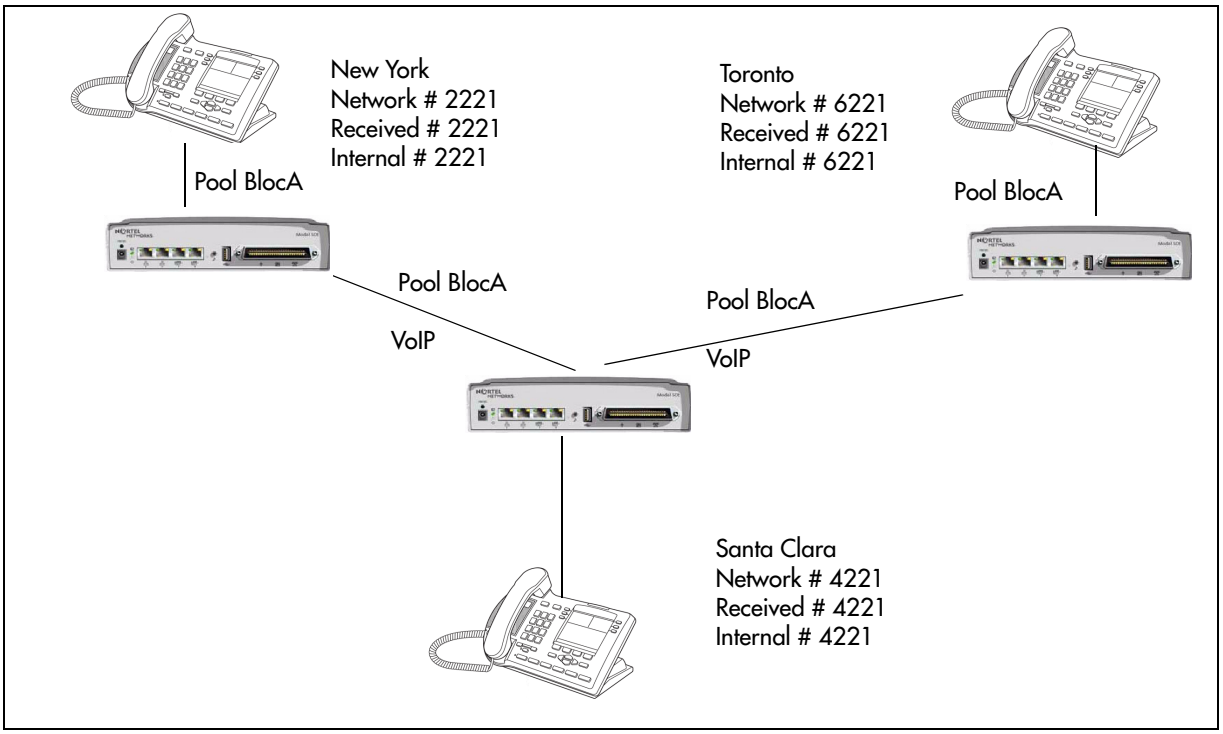
- Direct Inward Access (DIA) lines allow incoming calls on private circuits to be directed to telephones without going through the normal call reception. Each DIA line is assigned to one or more extensions and is given a distinct Private Received number. When someone on another system on the network dials the Private Received number on a DPNSS line, the BCM system checks all received digits, compares the digits to an internal table and routes the call to the appropriate DIA line. All extensions programmed to have access to that DIA line will then alert for the incoming call.
- Dialing restrictions can be added to lines in line pools. Filters can restrict the use of the line to specific area codes.
- You can use host system signaling codes (“External call codes” in the *Device Configuration Guide* (NN40020-300)) as part of the dial out for a route. Routing can also be used as an alternate method for a direct-dial digit. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1. Because overflow routing directs calls using alternate line pools, a call may be affected by different line restrictions when it is handled by overflow routing.

Chapter 37
Private networking: Using destination codes

By properly planning and programming routing tables and destination codes, an installer can create a dialing plan where VoIP lines between BCM are available to other systems in the network.

Figure 106 shows a network of three BCMs. Two remote systems connect to a central system.

Figure 106 Dialing plan for VoIP routing network



Each system must be running BCM software. Each system must be equipped with target lines and a VoIP keycodes with at least one IP Trunk line. Programming information for this network is shown in Table 72.

Table 72 VoIP routing for a BCM network (Sheet 1 of 3)

New York office:	
Parameter	**Setting**
Line Programming	
Network line (external)	
Line 001-004	VoIP
Line type	BlocA
Target line (internal)	
Line 125	Target line

Table 72 VoIP routing for a BCM network (Sheet 2 of 3)

Private Received #	2221	
Line Access (set)		
Set 2221	L125: Ring only	
Line pool access	Line BlocA	
Routing service		
Route	001	
Use	BlocA	
External #	None	
Routing Destinations	**Office #1**	**Office #2**
Routing to	Santa Clara	Toronto
Destination Code	4	6
Normal route	001	001
Absorb	None	None
Dialed number:	4221	6221

Santa Clara office:

Parameter	**Setting**	
Network line (external to New York)		
Line 001-004	VoIP	
Line type	BlocA	
Target line (internal to Santa Clara telephone)		
Line 125	Target line	
Private Received #	4221	
Line Access		
DN 4221	L125: Ring only	
Line pool access	Line BlocA	
Routing Destinations	**Office #1 and #2**	
Routing to	New York/Toronto	
Route	001	
Use	BlocA	
External #	None	
Destination Code	2	6
Absorb	None	None
Normal route	001	001
Remote access		**Note:** All lines in BlocA and BlocB need to be assigned in Remote Access Package 1. This is done under the restrictions tab of the lines.
Rem access pkgs	01	
Line pool access	BlocA: ON	
Line pool access	BlocB: ON	

Table 72 VoIP routing for a BCM network (Sheet 3 of 3)

Toronto office:		
Parameter	**Setting**	
Trunk/Line Data (external)		
Line 001-004	VoIP	
Line type	BlocA	
Target line (internal)		
Line 125	Target line	
Private Received #	6221	
Line Access		
DN 6221	L125: Ring only	
Line pool access	Line BlocA	
Routing Destinations	**Office #1**	**Office #2**
Routing to	New York	Santa Clara
Route	001	
Use	BlocA	
External #	None	
Destination Code	4	2
Absorb	None	None
Normal route	001	001

If a user in New York wants to call Toronto within the network, they dial 6221. The local BCM checks the number against the routing tables and routes the call according to the destination code 6, which places the call using Route 001.

The call appears on the routing table on the BCM in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 001 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line Private received number. The call now alerts at telephone 6221 in Toronto.

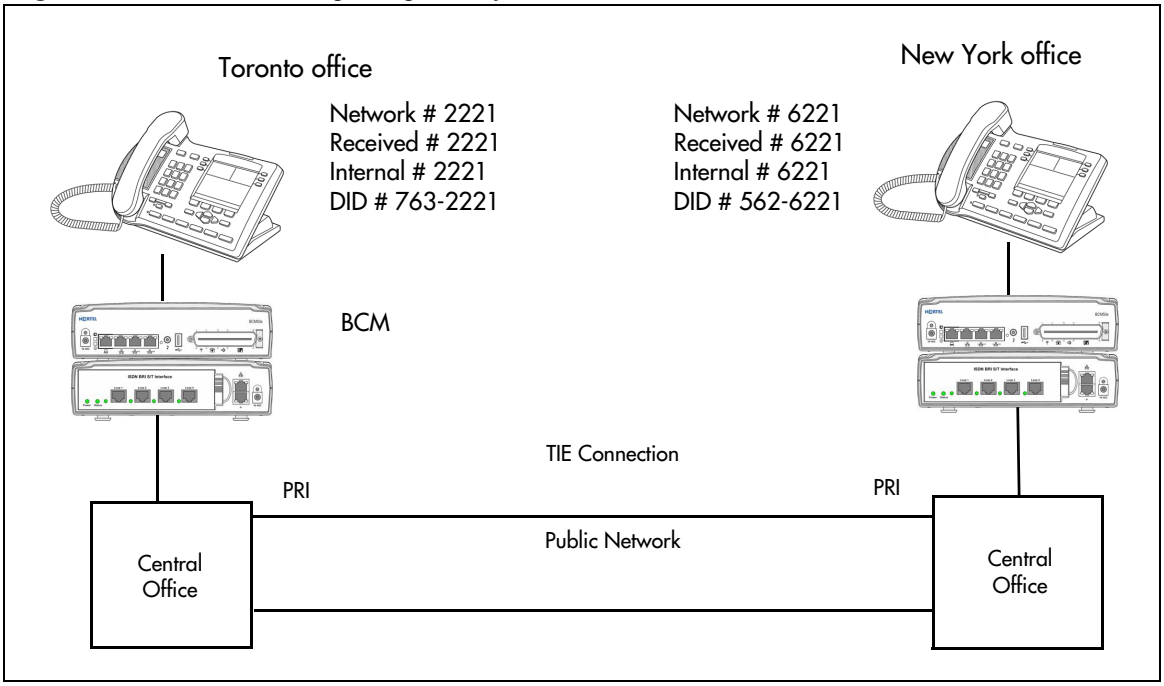
Note: Network calls that use routes are subject to any restriction filters in effect.
If the telephone used to make a network call has an appearance of a line used by the route, the call will move from the intercom button to the Line button.
The telephone used to make a network call must have access to the line pool used by the route.
Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.
When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal telephone numbers.
Routes generally define the path between your BCM and another call server in your network, not other individual telephones on that call server.

Chapter 38
Private networking: PRI Call-by-Call services

The example shown in Figure 107 highlights the use of PRI Call-by-Call services. It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with a BCM and a PRI line. Each office must handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office.

Note: Call-by-Call Services must be provided by the Central Office for them to work in the BCM.

Figure 107 PRI networking using Call-by-Call Services



To reduce long distance costs, and to allow for a coordinated dialing plan between the offices, private lines are used to handle interoffice traffic. Refer to "Dialing plan: Public network" on page 275 and "Dialing plan: Private network settings" on page 281.

If Call-by-Call services were *not* used, each BCM system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic
- eight T1 E&M lines needed to handle inter-office calls
- eight lines needed to handle outgoing public calls

The total required is thus 28 lines. If the BCM systems were using T1 trunks, then two T1 spans would be required at each office. Note that the total of 28 lines represents the worst case value for line usage. In reality, the total number of lines in use at any one time will generally be less than 28. For example, during periods of peak incoming call traffic, the demand for outgoing lines will be low.

With PRI Call-by-Call services, it is not necessary to configure a fixed allocation of trunks. Each of the 23 lines on the PRI can be used for DID, private TIE, or outgoing public calls. This consolidation means that it may be possible for each office to use a single PRI span, rather than two T1 spans. With PRI Call-by-Call services, the only limitation is that there are no more than 23 calls in progress at any one time.

The dialing plan at each BCM site is configured to determine the call type based on the digits dialed by the user. If a user in Toronto wishes to dial a colleague in New York, they dial the four-digit private DN (such as 6221). The dialing plan recognizes this as a private network DN, and routes the call using TIE service with a private dialing plan.

Incoming TIE calls are routed to telephones based on the digits received by the network, which in this case will be the four-digit private DN.

If a user in either location wishes to dial an external number, they dial 9, followed by the number (such as 9-555-1212). The dialing plan recognizes this as a public DN, and routes the call using Public service.

Incoming DID calls will be routed to telephones, based on the trailing portion of the digits received by the network. For example, if a public network user dials an employee in the Toronto office, the network delivers digits 4167632221. The BCM routes the call using the last four digits, 2221, to the BCM50.

Refer to Table 73 for a description of the settings required for this type of routing service.

Table 73 PRI Call-by-Call services routing information (Sheet 1 of 2)

Parameter	Home System Settings	
Hardware		
DTM	PRI	
Protocol	NI-2	
Trunk/Line Data		
Line 125	Target line	
Private/Public Received #	2221	
Line Access		
DN 2221	L125:Ring only	
Line pool access	Line pool BlocA	
Routing Services	**Private Network**	**Public network**
	New York:	**Public network**
Route	001	002
External #	No number	No number
Use	Pool BlocA	Pool BlocA
Service type	TIE	Public

Table 73 PRI Call-by-Call services routing information (Sheet 2 of 2)

ServiceID	1	N/A
DN type	Private	N/A
Destination Code	6	9
Normal route	001	002
Absorb	0	ALL

New York office:

Parameter	**Home System Settings**
Hardware	
DTM	PRI
Protocol	NI-2
Trunk/Line Data	
Line 125	Target line
Private/Public Received #	6221
Line Access	
DN 6221	L125:Ring only
Line pool access	Line pool BlocA

Routing Services	**Private Network**	**Public Network**
	Toronto	Public Network
Route	001	002
External #	No number	No number
Use	Pool BlocA	Pool BlocA
ServiceType	TIE	Public
ServiceID	1	N/A
DN type	Private	N/A
Destination Code	2	9
Normal route	001	002
Absorb	0	ALL

Chapter 39
Configuring voice messaging

You can have either an internal voice message service, or you can connect your system to an external voice message service, either over the PSTN network to a message center at the central office or through a private network to another system. This panel allows you to choose the type of voice messaging service you want to use. If you choose an external service, you can enter the contact numbers to the Centralized Voice Messaging table.

The following paths indicate where to access the loop start trunks through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Applications > Voice Messaging > Contact Center**
- Telset interface: ****CONFIG > Telco features**

Assign external numbers to System Speed dial codes.

Panels/Subpanels	Tasks/features
“Centralized Voice Messaging (external voice mail)” on page 347	“Configuring centralized voice mail” on page 351
“Local voice messaging access (CallPilot Manager)” on page 349	Refer to the CallPilot documentation for task and feature details.
Click the navigation tree heading to access general information about Hospitality services.	

Centralized Voice Messaging (external voice mail)

This panel allows you to record on the system the dial strings that allow users on your system to access a remote voice messaging service. Note that public or private trunks need to be properly configured for these numbers to work.

Figure 108 Voice Message Centers table

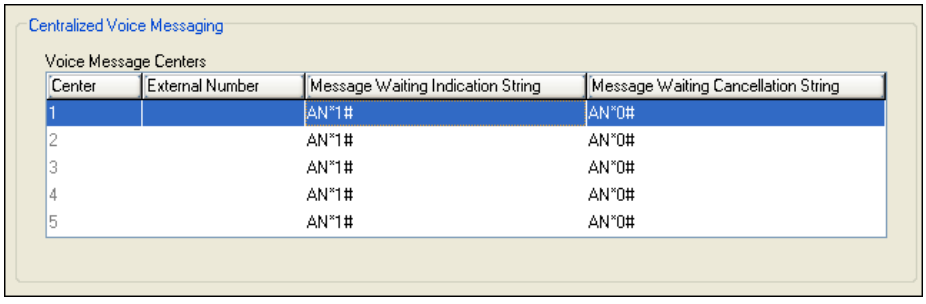


Table 74 describes each field on this panel.

Table 74 Voice Message Centers Table

Attribute	Values	Description
Center	<read-only>	You can define a maximum of five external voice message centers. Note that any one user can only be connected to one center.
External Number	<dial string>	This is the number for the external voice message center. Ensure that you add the appropriate routing information.
Message wait indicate string (MWI)	<string>	Indicates that the message center has a message in the mailbox. This is a default NSI string for message waiting. Refer to "Programming MWI and MWC strings" on page 348.
Message wait cancellation string (MWC)	<string>	Indicates that the voice messages have been retrieved. This is a default NSI string for message waiting.

Programming MWI and MWC strings

MWI and MWC information is received from the network in the form of NSI strings.

The default MWI and MWC strings are default NSI strings for Message Waiting.
*58B*AN*1# – Message Waiting Indication
*58B*AN*0# – Message Waiting Cancellation
This provides the information required to program the strings as:
AN*1# for MWI, and
AN*0# for MWC
Private network strings will differ with different message centers. These should only be changed on the advice of your customer service representative.

DPNSS: The NSI strings in DPNSS are dependent on the supplier of the PBX. Therefore, the strings vary depending on the originating PBX system.

Each string has the following default structure: *58XYYYYY.*

Table 75 describes each part of the NSI string.

Table 75 Parts of the NSI string

String Component	Description
`*58`	Identifies that it is an NSI string.
X	Any letter from A to Z, or nothing.
YYYYY..	Manufacturer specific string, which can contain any sequence of alphanumeric digits or *.
#	Marks the end of the identifier.

Only the `YYYYY.. #` portion of the string must be programmed for MWI and MWC. The procedure is similar to Set Name/Line Name.

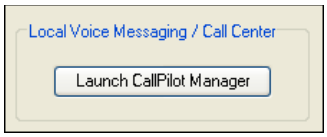
The following criteria must be met when programming NSI strings for MWI/MWC:

- No spaces are allowed, including spaces at the end of the string.
- A # must be present at the end.
- A # or a * cannot be present in the first character.

Local voice messaging access (CallPilot Manager)

Local voice messaging is configured using a client application. This CallPilot application is explained in detail in the CallPilot documentation.

Click the Launch CallPilot Manager button to access the application from which you can set up your local voice messaging system.



Chapter 40
Configuring centralized voice mail

The BCM supports voice-mail configuration either from the local source or by accessing a remote voice mail system located on another BCM, located on a BCM50, or attached to a Meridian 1 system. The system can be configured to more than one voice mail system. However, each telephone can only be configured to one system.

Refer to the following information:

- "Local system as host" on page 351
- "Meridian system as host" on page 352
- "System set up for host system" on page 352
- "System set up for satellite systems" on page 353
- "Configuring the system for centralized voice mail" on page 355

DMS-100/SL100 centralized voice mail: The BCM can also support centralized voice mail on a DMS-100/SL100 switch through a PRI-DMS-100 connection. The system also supports centralized voice mail on the switch through an indirect connection through an M1, where the DMS-100/SL100 is connected by PRI-DMS-100 to the M1, and the M1 is connected to a BCM through a PRI-MCDN connection. The DMS-100/SL100 can use either the Public number or Private number of a BCM telephone to designate the mailbox number on the voice mail system.

To configure centralized voice mail, the system must be using a CDP dialing plan and be running on a private network created using either DPNSS (UK profile), PRI SL-1 or VoIP trunking set up with MCDN. Private network configuration and features are discussed in "Private networking: MCDN over PRI and VoIP" on page 297.

Note: For centralized voice mail from a DMS-100/SL100 system, configure the BCM dialing plan as either CDP or UDP.

Local system as host

A local system that acts as a central voice-mail location must be able to support MCDN. You can add up to 1000 mailboxes on BCM voice mail, providing you have entered adequate keycodes.

CallPilot constraints:

- To allow use of the auto attendant feature, you must ensure that the **Allow Network Transfers** check box is selected in the CallPilot Manager.
- To allow use of voice mail, you must ensure that the **Enabled Redirected DN** check box is selected in the CallPilot Manager.
- A target line must be set up to be answered by the auto attendant. The target line received digits should match the voice mail DN.

For details about setting up the CallPilot parameters and features, refer to the *CallPilot Manager Set Up and Operations Guide* and the other CallPilot supporting documentation.

Meridian system as host

If you are using a voice mail system connected to a Meridian 1 as a host system, ensure that the systems are set up to be compatible with each other.

CallPilot compatibility

If you are planning to use M1-based CallPilot software for the voice mail system, there are no compatibility issues.

Note: CallPilot for BCM accepts network-wide and site-specific VPIM broadcast messages from M1 CallPilot, if the VPIM prefix in the message address matches the local mailbox prefix.

Meridian Mail compatibility issues

If you are using Meridian Mail as the host system, ensure that the Meridian has the following:

- Meridian Mail rel. 7 (MM7) or above
- the appropriate number of PRI cards and D-channel handlers to support the PRI links to all the BCMs using the system.

Special requirements:

- Over a PRI SL-1 line: Meridian 1 must be on Release 19 or greater.
- Over VoIP: Meridian one must be installed with an IPT card version 3.0 or newer
- Meridian 1 requires the network ID of the BCM, select **Configuration > Telephony > Dialing Plan > Private Network** in the Element Manager. The ID is a number between 1 and 27, and is defined by the Meridian system administrator.

Also refer to "System set up for satellite systems" on page 353 for specific call features available from a Meridian 1-based voice mail system.

System set up for host system

The system that hosts the voice mail needs to ensure that incoming calls are directed to the voice mail service.

Process assumptions:

- Private network is set up, with MCDN, between any nodes that need to access voice mail on this system.
- All systems are using the CDP dialing plan, and you have set up the correct routing to these systems.

- CallPilot or auto attendant is set up and is running for the local system.
- You have obtained a list of DNs from the remote systems that require mailboxes.

To configure the host system

1. Obtain the voice mail DN by pressing **FEATURE 985** on a system telephone.
2. If this setting matches the DN scheme for your system dialing plan, go to step 3.

   If this setting does not match the DN scheme for your system dialing plan:

   a. To access the DNs panel, select **Configuration > Telephony > Dialing Plan**.

   b. In the All DNs table, locate the DN to be changed.

   c. Double-click the number in the DN column.

   d. Enter the number obtained in step 1.
3. To access the Target Lines panel, select **Configuration > Telephony > Lines**.
4. In the Target Lines table, locate the target line to be assigned.
5. In the Details for Line subpanel, click the Assigned DNs tab.
6. Click **Add**.
7. Enter the required DN in the DN field.
8. Click **OK**.

CallPilot programming:

9. Set up CallPilot for voice mail or auto attendant answering:
   - **Voice mail:** In CallPilot Manager, click **Configuration**, and the click **System Properties**. Ensure that the **Enable Redirected DN** box is selected.
   - **Auto-Attendant:** Under the **Auto-Attendant** heading, click the line record you specified in step 4 and set the Auto-Attendant to answer after 0 (zero) rings.

VoIP networking note: If you are using H.323 VoIP trunks for central voice mail, you need to set the following:

- Ensure that the local gateway protocol is set to SL-1 or CSE, based on the version of the satellite systems.
- Ensure that the remote gateways are programmed to route using CDP.
- Ensure that the remote gateway protocols are set to SL-1 or CSE, based on the version of the satellite system.

System set up for satellite systems

Systems that are remote to the voice mail system need to ensure that outgoing calls are correctly directed to the voice mail service on the host system.

Process assumptions:

- Private network has been set up, with MCDN, between the satellite and host system.
- The correct routing to the host system is set up and working.
- You have supplied a list of DNs to the host system administrator that require mailboxes.

To set up a satellite system for voice mail

1. To access the Centralized Voice Messaging panel, select **Configuration > Applications > Voice Messaging / Contact Center**.
2. Click the voice center number that you want to assign to the remote voice mail system.
3. In the External Number field, enter the voice mail DN assigned by the host system. Ensure that you include any appropriate routing codes to the string.

   Also refer to Centralized Voice Messaging (external voice mail) in the *Device Configuration Guide* (NN40020-300).

   DPNSS process: Type the new target number, starting with an access code, if required, or **None**. For example: **65142222**.
4. Enter the Message Waiting Indication String that is expected from the particular message center.
5. Program the Message Waiting Cancellation String that is expected from the message center.

Note: The line must be programmed to Appear and/or Ring at the telephone.

Configuring the Target lines:

6. If the telephone does not already have a target line assigned:
   a. To access the Target Lines panel, select **Configuration > Telephony > Lines > Target Lines**.
   b. In the Target Lines table, locate the target line to be assigned.
   c. In the Details for Line subpanel, click the Assigned DNs tab.
   d. Click **Add**.
   e. Enter the required DN in the DN field.
   f. Click **OK**.
   g. Click the **Preferences** tab.
   h. In the Voice message center field, enter the center number of the voice center number that you want to assign to the remote voice mail system.
7. Repeat the previous step for all the target lines you want to change.

Configuring the telephone records:

8. To access the DNs panel, select **Configuration > Telephony > Sets > All DNs**.
9. In the All DNs table, click the DN you associated with the voice mail target line.

10 In the Details for DN subpanel, click the Line Assignment tab.

11 Add the line number of the target line programmed for the telephone.

12 Select the **Vmsg** check box.

Configuring Call forward to go to voice mail:

13 For the same DN:

- a Click the **Capabilities and Preferences** tab.
- b In the Details for DN subpanel, select the **Allow redirect** check box.
- c Click the Line Access tab.
- d Double-click the **Fwd No Answer** field.
- e Enter the voice mail DN.
- f Double-click the **Fwd Busy** field.
- g Enter the voice mail DN.

14 Repeat the previous step for each of the DNs you want to assign to the remote voice mail.

15 Test the system.

VoIP networking note: If you are using H.323 VoIP trunks for central voice mail, you need to set the following:

- Ensure that the local gateway protocol is set to CSE, based on the version of the satellite systems.
- Ensure that the remote gateways are programmed to route using CDP.
- Ensure that the remote gateway protocols are set to CSE, based on the version of the satellite system.

16 Repeat for each center you want to identify.

TIPS:

- A telephone does not show that external voice messages are waiting unless you enable **VMSG set** for the lines assigned to each telephone under **Line Assignment**. Refer to “Capabilities tab” in the *Device Configuration Guide* (NN40020-300).
- Analog telephones connected to an GASM can receive message waiting indicators if the analog line supports CLID. MWI indicator settings for analog telephones or for analog telephones attached to ATA2s, are set under the ATA heading “Configuring an analog telephone” in the *Device Configuration Guide* (NN40020-300).
- You can program up to five voice message center numbers, but many systems require only one.

Configuring the system for centralized voice mail

MCDN is supported over a PRI (SL-1) line or VoIP trunks between your BCM and other systems, such as Meridian 1, or Business Communications Manager systems. The following describes the specific programming for remote voice mail over PRI lines.

Apart from line configuration, MCDN over VoIP has the same system configuration.

To set up a PRI connection on the system

1. Ensure that the remote voice mail system is set up to accommodate your system on the network.
2. Ensure that your dialing plan coordinates with what the other nodes on the network are using. (select **Configuration > Telephony > Dialing Plan > Private network ID**)
3. Enter the network system identifier the Meridian system administrator supplied (between 1 and 127), if you are networked with a Meridian 1 somewhere in the network. (select **Configuration > Telephony > Dialing Plan, Private Network panel, Private network type**)
4. Install a DTM module to connect to the appropriate PRI SL-1 trunk, or enter the keycode for the required number of VoIP trunks.
5. Configure the lines you plan to use, assigning them to the same line pool. Refer to "Configuring lines: PRI" on page 145 and "Configuring VoIP lines" on page 385.
6. Enter the MCDN keycode.
7. Choose the MCDN network features that you want to use. (Select **Configuration > Telephony > Dialing Plan, Private Network** panel, and then select the MCDN subpanel)
8. Set up routing to target the PRI or VoIP line pool you set up.
9. Set up your dialing plan to recognize the network system identifiers of the other nodes on the system, so your system can pass them along, as required.
10. Assign the pool to any telephones you want to allow to use this line.
11. Program target lines and assign to telephones.
12. Set up the voice mail DN for the system that is being used as the host voice mail system for your network.
13. Test the link.
14. Refer to the CallPilot documentation to set up the mailboxes or auto attendant features and other voice mail parameters.

Chapter 41
Dialing plan: Line pools and line pool codes

The Line Pools panels allow you to:

- assign access codes to line pools
- add lines to line pools
- assign lines pools to telephones (and view which telephones have line pool assigned)
- set Call-by-Call limits for PRI service types

The following paths indicate where to access line pools settings in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Line Pools**
- Telset interface: ****CONFIG > System Prgrming > Access Codes > Line pool** codes

Click one of the following links to connect with the type of information you want to view:

Panels	Tasks	Features and notes
"Line pools (and access codes)" on page 357 "Line pools: DNs tab" on page 359 "Line pools: Call-by-Call Limits tab (PRI only)" on page 360		"Line pool access code notes:" on page 358

Also refer to:

- "Configuring lines" on page 129
- "Dialing plan: Routing and destination codes" on page 259
- "Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300)

Click the navigation tree heading to access general information about DN records.

Line pools (and access codes)

The panel in the top frame displays settings that are configured on other panels. The only setting you can modify on this table is the access code number. Figure 109 illustrates this panel.

Figure 109 Dialing Plan - Line Pools table

Table 76 describes the fields on the top frame.

Table 76 Line Pools table fields

Attribute	Value	Description
Pool	<read-only>	These are the available line pools. Program only the ones for which you have actually assigned lines. Line pools are configured on the Lines panel
Access Code	<XXX>	Use access codes if you are not using destination codes on the system. These codes serve the same purpose, without the ability to define dialing sequences and multiple codes per route.

Line pool access code notes:

Note: You cannot assign Bloc line pools with a line pool access code. You must define Bloc line pools under routing, and create destination codes for the routes.

Note: A line pool access code cannot conflict with the following table.

Note: The line pool number must not conflict with the following:

- park prefix
- external code
- direct dial digits
- private access code
- Public/Private Auto DN
- Public/Private DISA DN
- Telephone DN

If the line pool code and the external code start with the same digit, the line pool code programming supersedes the external code.

Line pools: DNs tab

The DNs tab shows you which DNs have this line pool assigned.

Programming note: A line pool must be assigned to a telephone before the user can use the line pool access code (or destination code) to make a call.

Figure 110 illustrates the DNs tab.

Figure 110 DN access to line pools

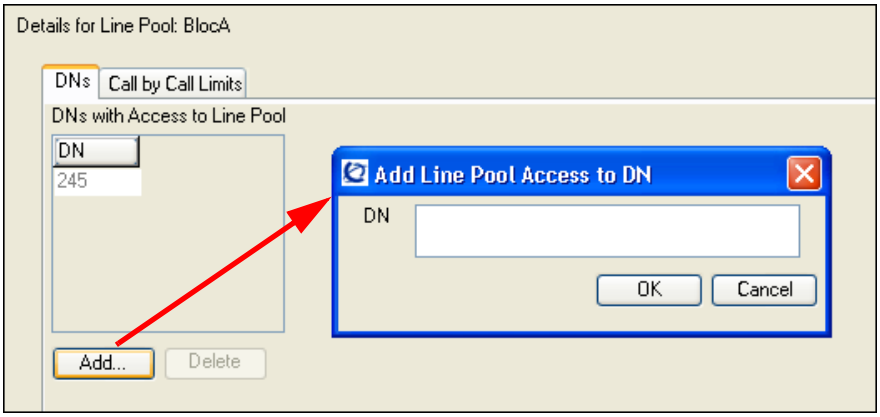


Table 77 describes the fields on the DNs tab.

Table 77 Line Pools: DN access to line pools fields (Sheet 1 of 2)

Attribute	Value	Description
DNs	<read-only>	The telephones assigned to the line pool. Also refer to: Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300).
Actions:		
Add	1. On the Line Pools table, select the line pool you want to modify. 2. Under the DNs tab table, click **Add**. 3. Enter the DN you want to assign to the line pool. 4. Click **OK** to save.	

Table 77 Line Pools: DN access to line pools fields (Sheet 2 of 2)

Attribute	Value	Description
Delete	1. On the Line Pools table, select the line pool you want to modify. 2. On the DNs tab table, select the DN you want to delete. 3. Under the DNs tab table, click **Delete**. 4. Click **OK**.	

Line pools: Call-by-Call Limits tab (PRI only)

For PRI lines that provide Call-by-Call services, Bloc line pools have an additional configuration that allows you to configure service type limitations. For information on PRI protocols, refer to Table 42.

Figure 111 illustrates the Call-by-Call Limits tab.

Figure 111 Line Pools: Call-by-Call Limits fields

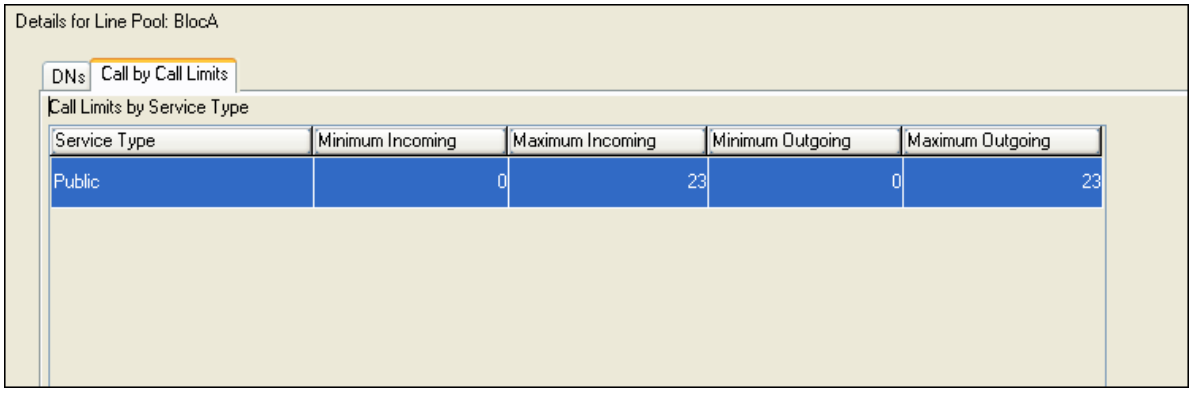


Table 78 describes the fields on the Lines tab.

Table 78 Line Pools: Call-by-Call limits fields

Attribute	Value	Description
Service Type	<read-only>	This is the type of CbC service provided on the PRI trunks in the line pool.
Minimum Incoming	Default: 2	**Note**: The total of the minimum values for incoming or outgoing PRI services cannot exceed the total number of lines in the Blocpool. The maximum value for an incoming or outgoing PRI service cannot exceed the total number of lines in the Bloc pool.
Maximum Incoming	Default: 23	
Minimum Outgoing	Default: 4	
Maximum Outgoing	Default: 23	

Chapter 42
VoIP overview

On the BCM, the LAN configuration consists of two components: Router LAN configuration, which determines how the router communicates with devices on the LAN, and Main Module LAN configuration, which determines how the Main Module of the BCM communicates with other devices on the LAN.

IP telephones

IP telephones offer the functionality of regular telephones but do not require a hardwire connection to the BCM. Instead, they must be plugged into an IP network, which is connected to the LAN or WAN on the BCM. Calls made from IP telephones through the BCM can pass over VoIP trunks or across a Public Switched Telephone Network (PSTN).

Nortel has several types of IP telephones that connect to the BCM through Ethernet. The IP softphone 2050, which runs as a client application on a PC or PDA, also connects to the BCM through the Ethernet.

VoIP trunks

VoIP trunks allow voice signals to travel across IP networks. A gateway within the BCM converts the voice signal into IP packets, which are then transmitted through the IP network to a gateway on the remote system. The device at the other end reassembles the packets into a voice signal.

Creating an IP telephony network

An IP telephony network consists of telephones, gatekeepers, IP networks, and access to a PSTN.

Networking with BCM

The BCM is a key building block in creating your communications network. It interoperates with many devices, including the Meridian 1 system and BCM devices. The BCM system can be connected to devices through multiple IP networks, as well as through the PSTN. Multiple BCM systems also can be linked together on a network of VoIP trunks and/or dedicated physical lines.

Telephones

The BCM can communicate using digital telephones (7000, 7100, 7100N, T7208, 7208, 7208N, 7316, 7316E, 7316E+KIMs, and 7310), cordless telephones (7406), and IP telephones and applications (Nortel IP Phone 2001, IP Phone 2002, IP Phone 2004, and Nortel IP softphone 2050). With this much flexibility, the BCM can provide the type of service you require to be most productive in your business.

Note: Model 7000 phones are supported in selected markets only.

While analog and digital telephones cannot be connected to the BCM system using an IP connection, they can make and receive calls to and from other systems through VoIP trunks. Calls received through the VoIP trunks, or other IP telephones, to system telephones are received through the LAN or WAN card and are translated within the BCM to voice channels.

Gatekeepers

A gatekeeper tracks IP addresses of specified devices, and provides routing and (optionally) authorization for making and accepting calls for those devices. A gatekeeper is not required as part of the network to which your BCM system is attached, but gatekeepers can be useful on networks with a large number of devices.

When planning your network, be sure to consider all requirements for a data network. Consult your network administrator for information about network setup and how the BCM fits into the network.

SIP Proxy

A SIP Entity that receives requests and sends them on to another proxy or to their final destination. A Proxy uses the information retrieved from the Location Service in order to find an alias or an actual destination address for the request. Alternatively, a Proxy can be statically configured, in which case registration is not necessary.

IP Network

WAN

A Wide Area Network (WAN) is a communications network that covers a wide geographic area, such as state or country. For CallPilot, a WAN is any IP network connected to a WAN card on the CallPilot system. This can also be a direct connection to another CallPilot system.

If you want to deploy IP telephones that will be connected to a LAN outside of the LAN that the BCM is installed on, you must ensure the BCM has a WAN connection. This includes ensuring that you obtain IP addresses and routing information that allows the remote telephones to find the BCM, and vice versa.

LAN

A Local Area Network (LAN) is a communications network that serves users within a confined geographical area. For BCM, a LAN is any IP network connected on the BCM system. Often, the LAN can include a router that forms a connection to the Internet. A BCM can have up to two LAN connections.

Key VoIP concepts

The following explains a few commonly used VoIP terms.

QoS

QoS (Quality of Service) is technology that determines the maximum acceptable amount of latency, and balances that with the quality of the VoIP connection. BCM and network routers use QoS to ensure that real time critical IP packets, such as voice packets, are given higher routing and handling priority than other types of data packets.

Silence suppression

Silence suppression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36% to 40% of a full-duplex conversation is active. When one party in the conversation is quiet for more than a few hundredths of a second, voice packet transmission is suppressed until the party starts talking again. This is half-duplex. There are important periods of silence during speaker pauses between words and phrases. By applying silence suppression, average bandwidth use is reduced by the same amount. This reduction in average bandwidth requirements develops over a 20-to-30-second period as the conversation switches from one direction to another. Refer to “Silence suppression” on page 529.

Codecs

The algorithm used to compress and decompress voice over IP networks and VoIP trunks is embedded in a software entity called a codec (COde-DECcode).

Refer to “Codec rates” on page 549 for a listing of the supported codes and their transmission rates.

- The G.711 Codec samples the voice stream at a rate of 64 kbps (kilo bits per second), and is the Codec to use for maximum voice quality. Choose the G.711 Codec with the companding law (alaw or ulaw) that matches your system requirements.
- The G.729 Codec samples the voice stream at 8 kbps. The voice quality is slightly lower using a G.729 but it reduces network traffic by approximately 80%.
- The G.723 Codec should be used only with third party devices that do not support G.729 or G.711.

Codecs with Silence Suppression, also referred to as VAD (Voice Activity Detection), make VAD active on the system, which performs the same function as having silence suppression active. Also refer to "Silence suppression" on page 529.

Note: You can only change the codec on a configured IP telephone if it is online to the BCM, or if Keep DN Alive is enabled for an offline telephone.

Proactive Voice Quality Management (PVQM)

Proactive Voice Quality Monitoring (PVQM) provides real-time notification in case of voice over IP call quality degradation, thus allowing you to monitor and manage calls on the network in real time. As a result, you can be aware of, and respond to, changing network conditions in a proactive way.

PVQM monitors a set of metrics which include:

- packet loss
- inter arrival jitter
- round trip delay
- Listening R

These metrics and supplementary information provide you with valuable insight into the real time quality of the call from the end-user perspective. This information gives an indication of the type of problem, and can be used to locate the source of the issue, thus accelerating the isolation and diagnostics phase of problem resolution.

In addition to packet loss, inter arrival jitter and round trip delay, PVQM monitors the "listening R" value. The R-Factor, as defined by ITU G.107 and IETF 3611, is a call quality index that assesses network impairments such as packet drops, jitter and round trip delay with consideration for the burstiness and recency of these impairments. The Listening R metric provides you with definitive answers about the actual QoS delivered to the telephone user. With this metric, you see the raw data (such as jitter or packet drop rate), and a summary of the effect of the data on the quality experienced by the user.

For example, a Warning Threshold for the listening R-value might be set at 80. When voice quality drops below this value as measured at the telephone set itself, an event is generated. The event notification is augmented with other valuable state information, such as network loss rate, average rate of discards due to jitter, average length of bursts, and presented as an alarm. Analysis of the alarms and supplementary information in the alarm description helps you identify and troubleshoot voice quality issues and proactively initiate responsive actions.

Refer to the *Administration Guide* (NN40020-600) for information on how to configure and use PVQM functionality.

Chapter 43
VoIP trunk gateways

You can use a VoIP trunk to establish communications between a BCM and a remote system across an IP network. Each trunk is associated with a line record (lines 001-012), and are configured in the same way that other lines are configured.

However, VoIP trunks have additional programming to support the IP network connection.

This system supports SIP trunks and H.323 trunks. Both types of trunks support connections to other BCMs, a central call server such as Succession 1000/M, and trunk-based applications. SIP trunks and H.323 trunks are assigned to a single Pool, and the routing decision to route calls via H.323 or SIP is made based on the routing modes of the two services (Direct/Gatekeeper/Proxy) and the combined routing table.

To access the Voice over IP (VoIP) trunk gateway in Element Manager, select:

- Element Manager: **Configuration > Resources > Telephony Resources > IP Trunks > Routing Table** tab

Configuring a VoIP trunk requires the following:

- "Pre-installation system requirements" on page 367
- "Keycodes" on page 368
- "H.323 network applications considerations" on page 368
- "SIP network applications considerations" on page 368

You can use VoIP trunks for calls originating from any type of telephone within the BCM system. Calls coming into the system over VoIP trunks from other systems can be directed to any type of telephone within the system.

You cannot program Auto DN or DISA DN for VoIP trunks; therefore, you cannot use CoS passwords to remotely access features on your system. The exception to this would be a tandemned call, where a call comes into system A over the PSTN, then tandems to system B over a VoIP trunk. In this case, the remote access package on the line will determine which system features are available to the caller.

Pre-installation system requirements

Ensure that you have obtained the following information or familiarize yourself with the requirements before continuing with VoIP trunk configuration:

Keycodes

Before you can use VoIP, you must obtain and install the necessary keycodes. See the *Keycode Installation Guide* (NN40010-301) for more information about installing the keycodes. Talk to your BCM sales agent if you need to purchase VoIP keycodes.

Each keycode adds a specific number of VoIP trunks. To activate trunking, you must reboot your BCM after you enter VoIP keycodes.

If you want to use the MCDN features on the VoIP trunks, you will need an MCDN keycode. If you have already deployed MCDN for your SL-1 PRI lines, you do not require an additional keycode.

H.323 network applications considerations

In order to maintain a level of quality during call setup, QoS monitor must be enabled and configured.

If your network uses a gatekeeper (H.323 trunks only), there are also specific settings that must be set on the H323 Settings panel to recognize the gatekeeper, and also within the gatekeeper application, so that VoIP lines are recognized. Also refer to gatekeeper configuration "VoIP interoperability: Gatekeeper configuration" on page 389.

If you plan to use H.323 trunking and you have a firewall set up, ensure that the ports you intend to use have been allowed.

SIP network applications considerations

In order to maintain a level of quality during call setup, QoS monitor must be enabled and configured.

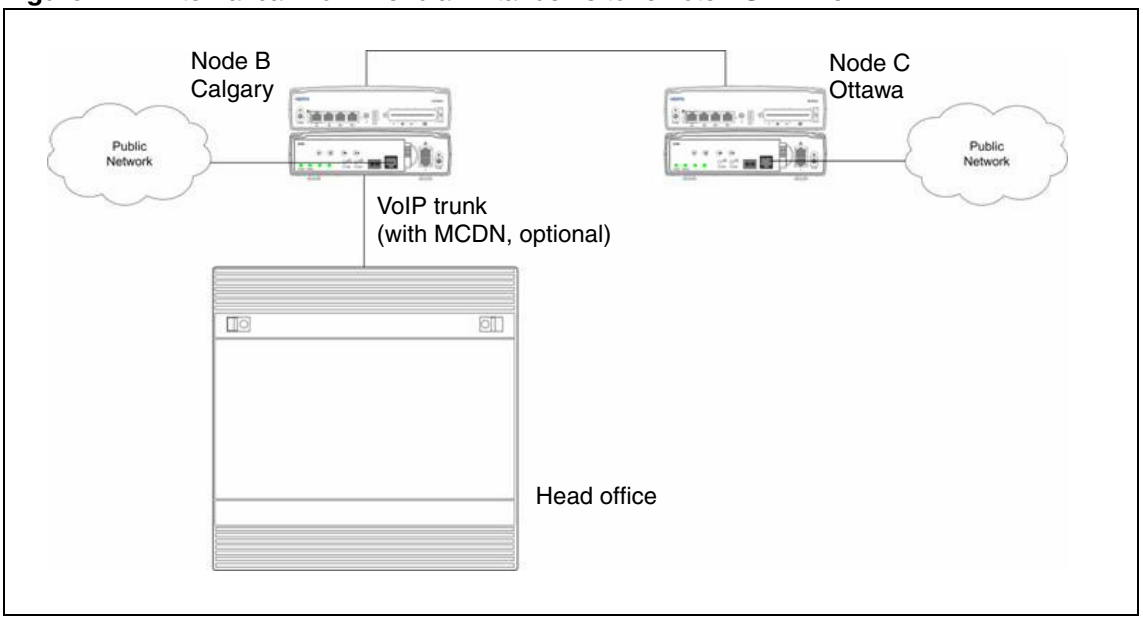
SIP URI maps of both endpoints must match.

If you plan to use SIP trunking and you have a firewall set up, ensure that the ports you intend to use have been allowed.

How VoIP trunks make a network

Figure 112 shows a simple private networking configuration of three systems connected by VoIP trunks. As in all private networking, each system has direct routing configurations to the directly adjacent systems. As well, the dialing plans are configured to ensure that remote calls are correctly routed to the receiving system, such as, if Node A called someone in Node C.

Figure 112 Internal call from Meridian 1 tandems to remote PSTN line



Since the VoIP trunks are configured into line pools, you can assign line pool codes to users who have been assigned access to the VoIP trunks. However, if you intend to set up your system to use fallback, so that calls can go out over PSTN if the VoIP trunks are not available, you must use routes and destination codes to access the VoIP trunk line pools.

Local gateway programming

The VoIP trunk access point at each system is called a gateway. The gateway to your system, the local gateway, determines how incoming and outgoing calls will be handled.

The H323 and SIP Media Parameters tabs determine a number of system settings. These values need to be coordinated with the other systems on the network to ensure that all features work consistently across the network. Media parameters include setting:

- the order of preferred codecs
- voice activity detection
- jitter buffer size
- codec payload size
- IP fax transmission availability on the network

The local gateway parameters define how the BCM prefers call signaling information to be directed through VoIP trunks. Call signaling establishes and disconnects a call.

If the network has a gatekeeper (H.323 trunks only), the BCM can request a method for call signaling, but whether this request is granted depends on the configuration of the gatekeeper. Ultimately, the gatekeeper decides which call signaling method to use.

Local gateway settings include:

- fallback to circuit switched availability and scope
- type of call signaling, either directly to the far end system or through a network gatekeeper
- if there is a gatekeeper, the relevant IP information is noted
- a KeepAlive signal timer
- the protocol the system will use for the gateway (must be compatible with remote system or gatekeeper)
- allowing/disallowing VoIP gateway tunnel H.245 messages within H.225
- being able to identify unique call signaling and RAS ports

Notes about NPI-TON aliases for H.323 trunks

NPI-TON aliases store dialed number prefixes as well as information about the type of number. A dialed number can be qualified according to its TON (type of number), as well as its NPI (numbering plan identification). Nortel recommends this format over the E.164 format, for encoding dialed numbers and aliases registered with a gatekeeper.

When using a gatekeeper, and attempting to place an outgoing VoIP trunk call, ensure that the route and dialing plan configuration matches the NPI-TON aliases registered, by the destination, with the gatekeeper. These requirements are summarized in Table 79.

Table 79 Route and Dialing Plan configurations for NPI-TON

Route (DN type)	Dialing Plan used by calling gateway	Alias configured for calling gateway ("alias name" in Element Manager)
Public	Public	PUB:<dialedDigitsPrefix>
Private	Private (Type = None)	PRI:<dialedDigitsPrefix>
	Private (Type = CDP)	CDP:<dialedDigitsPrefix>
	Private (Type = UDP)	UDP:<dialedDigitsPrefix>

Routing Table

Since VoIP trunks are point-to-point channels, besides the local gateway information on your system, you need to tell your system about the gateway at the remote end.

However, if the network has a gatekeeper or a SIP Proxy Server, it handles call traffic, so a routing table is not required.

To configure a remote gateway, you need to define the following information:

- a name that identifies the destination system

- the IP address of the destination system
- whether QoS monitor is enabled (this is required if you plan to use PSTN fallback)
- transmit threshold so that the system knows when to activate the fallback feature
- the remote gateway system type
- the gateway protocol
- the unique digit(s) that identify the remote system. (this is usually part of the destination code)

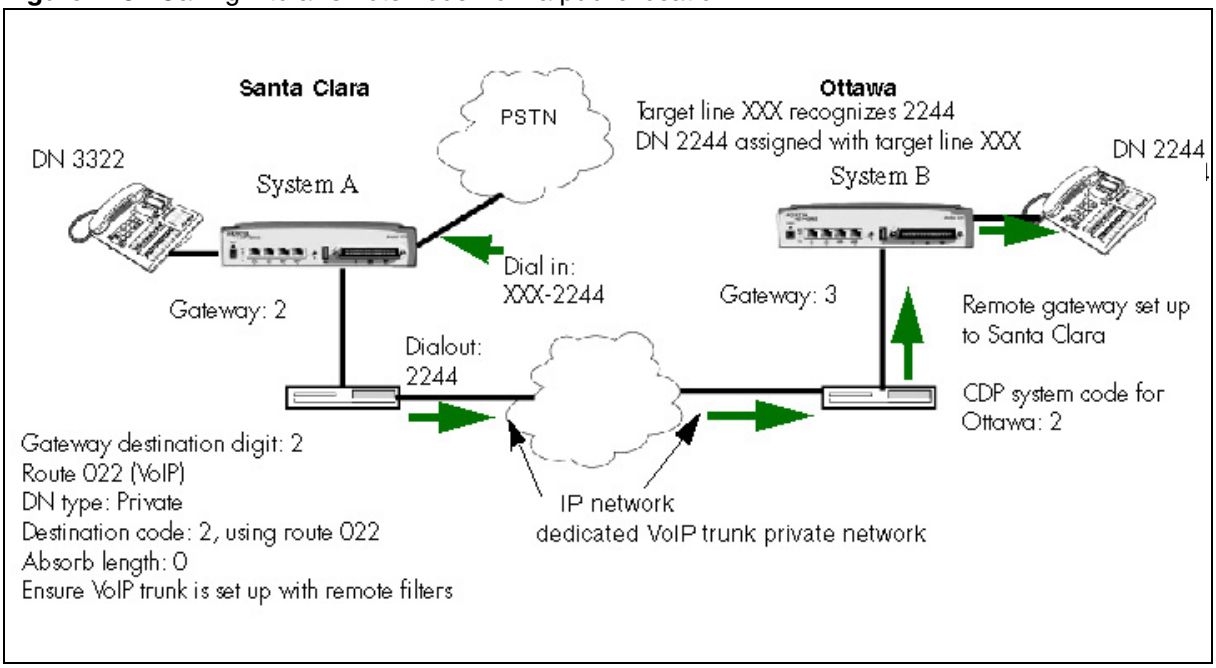
PSTN call to remote node

Making a call to a remote node requires any BCM systems between the calling and receiving nodes to have the correct routing to pass the call on to the next node. This is the same if you use PSTN lines or VoIP trunks for the network.

Figure 113 shows a call tandeming from the public network (PSTN), through System A (Santa Clara) and being passed to System B (Ottawa) over a VoIP trunk network. In this case, it might be a home-based employee who wants to call someone in Ottawa.

You cannot program DISA for VoIP trunks, therefore, your system cannot be accessed from an external location over a VoIP trunk. The exception to this is if the call comes into a tandemed system (system A) from a PSTN, and the call is then sent out across a VoIP trunk to system B, as in this example. In this case, system A is controlling remote access through remote access packages and routing, transferring the outside call to a VoIP trunk, which is accessed by an allowed dial sequence. The VoIP trunk connects directly to system B, where the dialing sequence is recognized as directed to an internal DN. In this scenario, all remote call features are available to the caller.

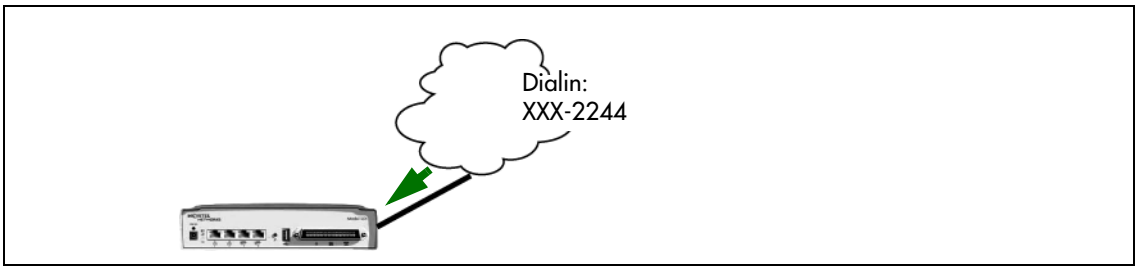
Figure 113 Calling into a remote node from a public location



Call process

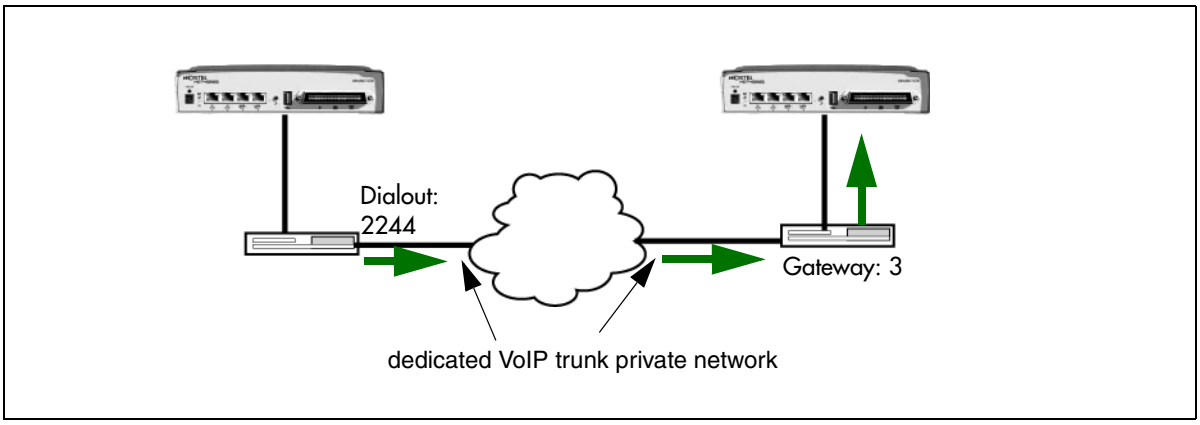
Based on Figure 113, this is how the call would progress:

1 A home-based employee in Santa Clara wants to call someone in Ottawa, so they dial into the local BCM network using the access code for an unsupervised trunk (not VoIP trunks) and the destination code and DN for the person they want to reach on System B.

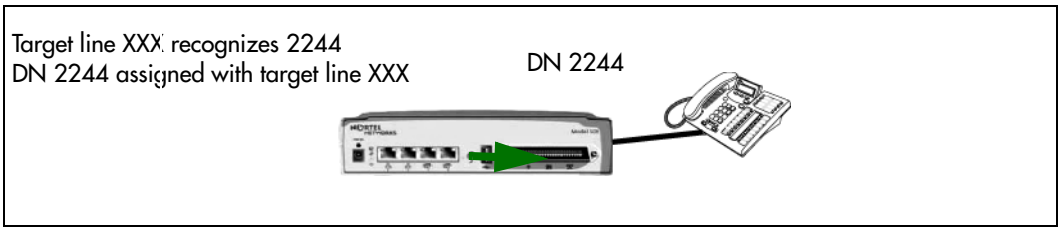


2 When the call is received from the public network at System A (Santa Clara), the system recognizes that the received number is not a local system number. The call is received as a public call.

3 System A has a route and destination code that recognizes the received number and destination code as belonging to the route that goes to System B (Ottawa). System A passes the call to System B over a dedicated trunk, in this case, a VoIP trunk. This call is now designated as a private call type.



4 System B recognizes the code as its own, and uses a local target line to route the call to the correct telephone.



Fallback to PSTN from VoIP trunks

Fallback is a feature that allows a call to progress when a VoIP trunk is unavailable or is not providing adequate quality of service (QoS).

Refer to the information under "Describing a fallback network" on page 374 for details about setting up fallback for VoIP trunks.

By enabling **Fallback to circuit-switched**, also known as PSTN fallback, on the H323 Settings or SIP Settings panels, you allow the system to check the availability of a VoIP trunk, then switch the call to a PSTN line, if the VoIP trunk is not available. For the PSTN fallback to work on a suitable bandwidth, QoS monitor must be enabled and a transmit threshold must be set. For QoS and transmit threshold settings refer to Table 81.

You use scheduling and destination codes to allow the call to switch from H.323 or SIP to a PSTN line without requiring intervention by the user.

Use the dialing plan worksheet in the Programming Records to plan your dialing requirements so you can pinpoint any dialing issues before you start programming. If you are programming an existing system, you can look at what numbers the users are familiar with dialing, and you can attempt to accommodate this familiarity into your destination codes plan.

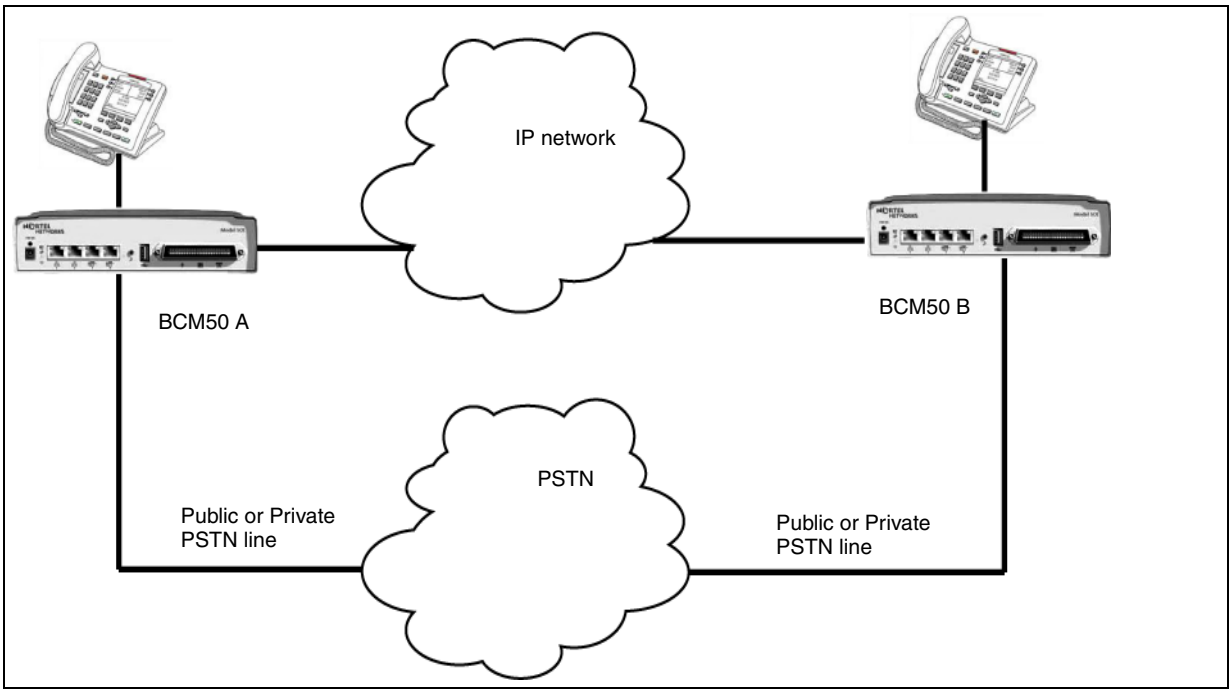
On any IP gateway for which you want to allow fallback based on network quality, you need to ensure that QoS monitor is enabled.

Warning: QoS monitor must be turned on at both endpoints. To enable the QoS Monitor select **Configuration > Resources > Telephony Resources > IP Trunks > Routing Table** panel.

Describing a fallback network

Figure 114 shows how a fallback network would be set up between two sites.

Figure 114 PSTN fallback diagram



In a network configured for PSTN fallback, there are two connections between a BCM and a remote system.

- One connection is a VoIP trunk connection through the IP network.
- The fallback line is a PSTN line, which can be the public lines or a dedicated T1, BRI, PRI or analog line, to the other system.

When a user dials the destination code, the system checks first to see if the connection between the two systems can support an appropriate level of QoS (if enabled). If it can, the call proceeds as normal over the VoIP trunk. If the minimum acceptable level of QoS is not met, the call is routed over the second route, through the PSTN line.

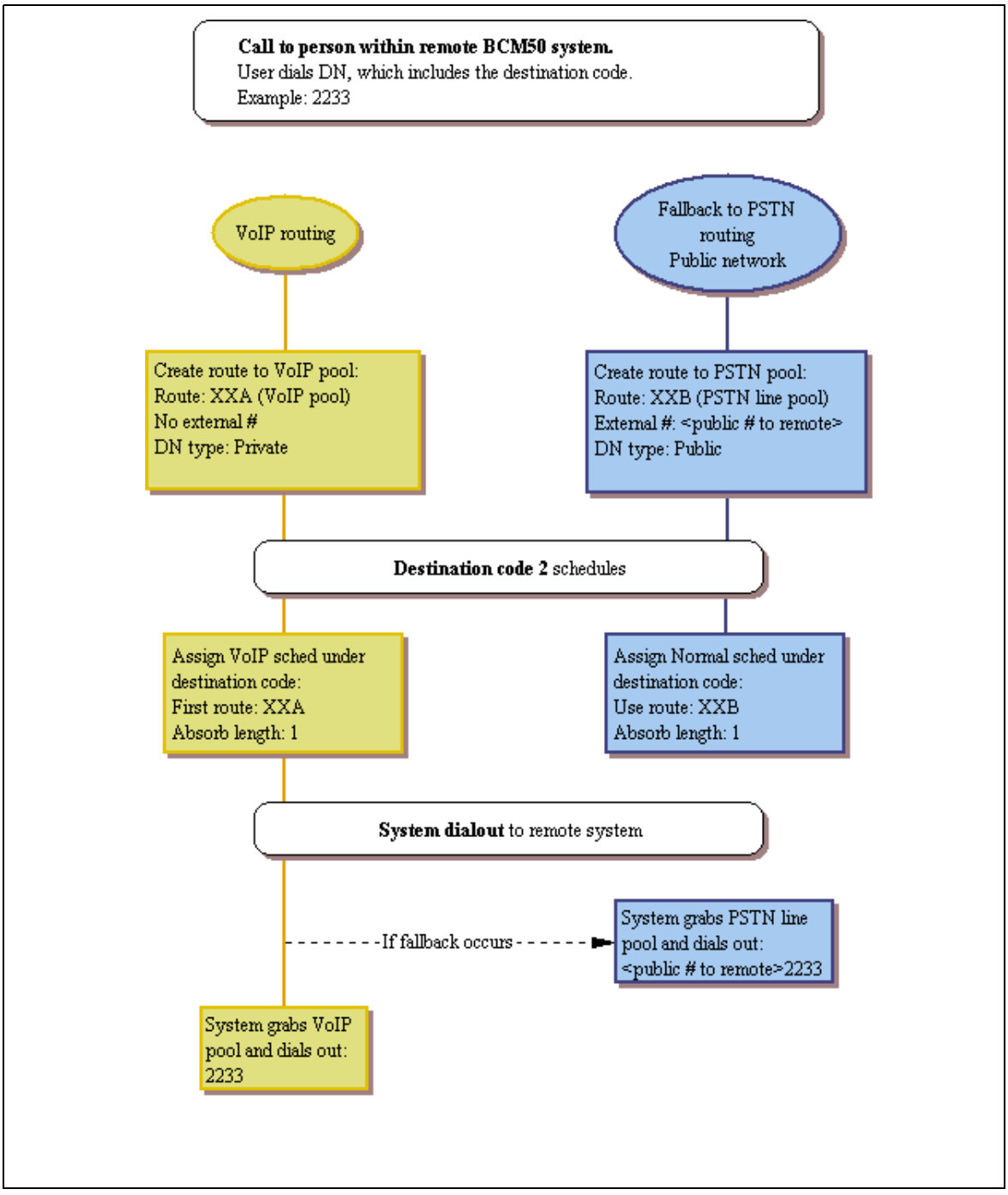
In many cases, this involves configuring the system to add and/or absorb digits.

For detailed information about inserting and absorbing digits, see "Dialing plans" on page 217.

How fallback routing works

CDP network: User dials 2233 (remote system DN: 2233; remote identifier/destination digit: 2). The system absorbs the 8, no other digits are absorbed and the system dials out 2233.
If the call falls back to PSTN line, the system still only absorbs the 8. If the PSTN line is on a private network, the system dials out 2233. If the PSTN line is a public line, the system dials out the public access number to the remote system in front of the 2233. Refer to Figure 115.

Figure 115 Setting up routes and fallback for call to remote system (CDP dialing code)


Call to person within remote BCM50 system.
User dials DN, which includes the destination code.
Example: 2233
VoIP routing
Fallback to PSTN routing
Public network
Create route to VoIP pool:
Route: XXA (VoIP pool)
No external #
DN type: Private
Create route to PSTN pool:
Route: XXB (PSTN line pool)
External #: <public # to remote>
DN type: Public
Destination code 2 schedules
Assign VoIP sched under destination code:
First route: XXA
Absorb length: 1
Assign Normal sched under destination code:
Use route: XXB
Absorb length: 1
System dialout to remote system
If fallback occurs
System grabs PSTN line pool and dials out:
<public # to remote>2233
System grabs VoIP pool and dials out:
2233

UDP network: The user dials 2233 (remote system DN: 2233; destination digits/private access code: 555). The system then adds the private access code to the dialout digits.
If the call falls back to PSTN line, the system then dials out the private access code (private network PSTN line) or public access number (public PSTN) to the remote system in front of the 2233.

Optional VoIP trunk configurations

A number of VoIP trunk features are optional to setting VoIP trunk functions. The following briefly describes these features:

- Port settings (firewall): In some installations, you may need to adjust the port settings before the BCM can work with other devices.

  Firewalls can interfere with communications between the BCM and another device. The port settings must be properly configured for VoIP communications to function properly. Using the instructions provided with your firewall, ensure that communications using the ports specified for VoIP are allowed.

  A Nortel IP telephone uses ports between 51000 and 51200 to communicate with the system. The system, by default, uses ports 28000 to 28255 to transmit VoIP packets.

  BCM uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. You must reserve these same port ranges and set them to high priority on all routers that an administrator expects to have QoS support. You do not need to reserve port ranges on DiffServ networks.

  You can select any port ranges that are not used by well-known protocols or applications.

  Each H.323 or VoIP Realtime Transfer Protocol (RTP) flow uses two ports, one for each direction. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

  — Include port number UDP 5000 in the reserved port ranges, for the QoS monitor.
  — The port ranges reserved in a BCM system are also reserved by the remote router.
  — You must reserve two ports for each voice call you expect to carry over the IP network.
  — You can reserve multiple discontinuous ranges. BCM requires that each range meet the following conditions: Each range must start with an even number; each range must end with an odd number; no more than 256 ports can be reserved.

Note: By default SIP uses port 5060.

- Gatekeepers: The BCM supports the use of an ITU-H323 gatekeeper. A gatekeeper is a third-party software application residing somewhere on the network, which provides services such as:
  — address translation
  — call control
  — admission control
  — bandwidth control
  — zone management
  — IP registration

A single gatekeeper manages a set of H.323 endpoints. This unit is called a Gatekeeper Zone. A zone is a logical relation that can unite components from different networks (LANS). These Gateway zones, such as the BCM, are configured with one or more alias names that are registered with the gatekeeper. The gatekeeper stores the alias-IP mapping internally and uses them to provide aliases to IP address translation services. Later, if an endpoint IP address changes, that endpoint must re-register with the gatekeeper. The endpoint must also re-register with the gatekeeper during the time to live (TTL) period, if one is specified by the gatekeeper.

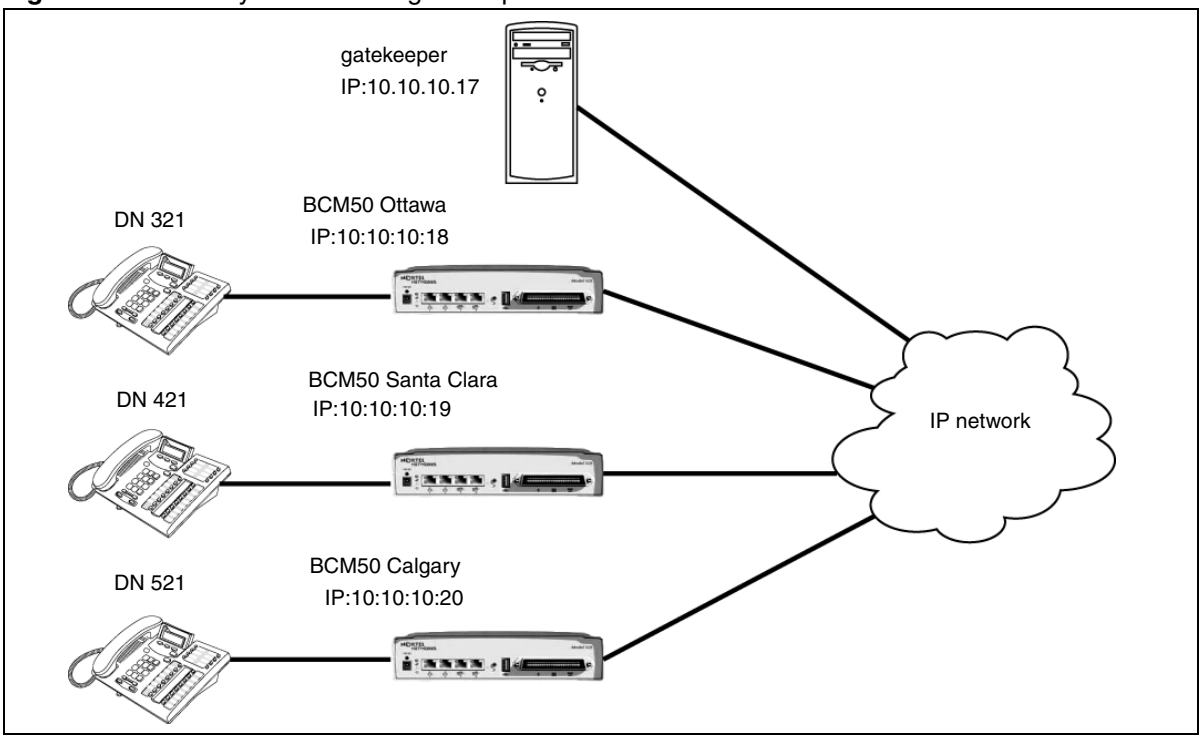
Refer to the gatekeeper software documentation for information about changing IP addresses.

Note: A gatekeeper may help to simplify IP configuration or the BCM dialing plan; however, it will not simplify the network dialing plan.

Gatekeeper call scenarios

The following explains how a call would be processed for the two types of gatekeeper configurations. Figure 116 shows a network with three BCMs and a gatekeeper.

Figure 116 BCM systems with a gatekeeper



This example explains how a call from DN 321 in Ottawa would be made to DN 421 in Santa Clara. It assumes that call signaling is set to Gatekeeper Resolved and no pre-granted AdmissionRequest (ARQ) has been issued:

1. BCM Ottawa sends an ARQ to the gatekeeper for DN 421.
2. The gatekeeper resolves DN 421 to 10.10.10.19 and returns this IP in an AdmissionConfirm to the BCM Ottawa.

3 BCM Ottawa sends the call Setup message for DN 421 to the gateway at 10.10.10.19, and the call is established.

If call signaling is set to Gatekeeper Routed and no pre-granted ARQ has been issued:

1 BCM Ottawa sends an ARQ to the gatekeeper for DN 421.

2 The gatekeeper resolves DN 421 to 10.10.10.17.

3 BCM Ottawa sends the call Setup message for DN 421 to the gatekeeper (10.10.10.17), which forwards it to the gateway at 10.10.10.19.

4 The call is established.

- Faxing over VoIP trunks: You can assign VoIP trunks to wired fax machines if you have T.38 fax enabled on the local gateway. The BCM supports this IP fax feature between BCMs, BCM200/400/1000 running BCM 3.5 and subsequent up-level versions of software, and a Meridian 1 running IPT 3.0 (or newer) software, or a CS 1000/M.

  The system processes fax signals by initiating a voice call over the VoIP line. When the T.38 fax packets are received at the remote gateway, the receiving system establishes a new path that uses the T.38 protocol. Both the endpoints must be running a software version that supports the T.38 fax.

Caution: Operations note: Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference:

- Locate fax machine away from other telephones.
- Turn the speaker volume on the fax machine to the lowest level, or off.

Fax tones recorded in a voice mailbox: In the rare event that fax tones are captured in a voice mail message, opening that message from an telephone using a VoIP trunk will cause the connection to fail.

For a list of limitations and requirements for using T.38 fax, refer to "Operational notes and restrictions" on page 379.

Operational notes and restrictions

Some fax machines will be unable to successfully send faxes over VoIP (T.38) trunks to the following destinations:

- CallPilot mailboxes
- CallPilot mailboxes (accessed through auto-attendant)
- Fax Transfer (calls transferred to a system fax device through the auto-attendant)
- Use the following tips to avoid this problem:

- Avoid the use of manual dial on the originating fax machine. In some fax machines, manually dialing introduces a much shorter call time-out.
- If manual dial must be used, then the user should wait until the call is answered before starting the fax session.
- If manual dial must be used, then the user should enter the digit **8** before initiating the fax session. This ensures that the fax session is initiated by CallPilot before the fax machine's timer is started.
- The call duration can be increased by adding a timed pause to the end of dialing string (for example: 758-5428,,,,). This allows the call to ring at the destination before the fax machine call duration timer starts.
- Since the problem is related to the delay in initiating the fax session, the number of rings for fax mailboxes Call Forward No Answer (CFNA) should be minimized.

Table 80 is a list of restrictions and requirements for the T.38 fax protocol.

Table 80 T.38 restrictions and requirements

Supported	Not supported
only UDP transport	TCP
only UDP redundancy	Forward Error Correction (FEC)
T.38 version 0	Fill removal
on H.323 VoIP trunks between BCMs, between BCMs and legacy BCMs, or between BCM and Meridian 1-IPT and CS 1000/M	MMR transcoding
	JBIG transcoding

Chapter 44
Configuring VoIP trunk gateways

The following explains how to configure voice over IP (VoIP) trunks on a BCM system for incoming traffic. A VoIP trunk allows you to establish communications between a BCM and a remote system across an IP network.

The following path indicates where to where to configure VoIP trunks in Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources > IP Trunks**

Task: Set up VoIP gateway parameters

- Set up the media parameters for the gateway. ("Configuring VoIP trunk media parameters" on page 382)
- Set up the local gateway parameters, including H323 gatekeeper or SIP Proxy settings, if necessary. ("Setting up the local gateway" on page 383)
- Set up the routing table, if one is required. ("Setting up remote gateways" on page 385)
- Configure the line parameters. ("Configuring VoIP lines" on page 385)

Prerequisites

Ensure that you have obtained the following information or familiarize yourself with the requirements before continuing with VoIP trunk configuration:

- Keycodes: Obtain and install the necessary keycodes for the number of VoIP trunks you want to support on the system. See the *Keycode Installation Guide* (NN40010-301) for more information about installing the keycodes. Talk to your BCM sales agent if you need to purchase VoIP keycodes.

  Each keycode adds a specific number of VoIP trunks. You must reboot your BCM after you enter VoIP keycodes to activate trunking.

  The FEPS service will restart automatically after you enter the VoIP keycodes.

  If you want to use the MCDN features on the VoIP trunks, you will need an MCDN keycode. If you have already deployed MCDN for your SL-1 PRI lines, you do not require an additional keycode.

- Media gateway parameters: Ensure that the gateway parameters are set correctly for the IP trunks.

- H.323 network applications considerations:

— If your network uses a gatekeeper (H.323 trunks only), there are also specific settings that must be set on the your system to recognize the gatekeeper, and also within the gatekeeper application, so that VoIP lines are recognized. Refer to "VoIP interoperability: Gatekeeper configuration" on page 389. If there is a gatekeeper on the network, you do not have to configure remote gateway settings.

— If you plan to use H.323 trunking and you have a firewall set up, ensure that the ports you intend to use have been allowed.

- SIP network applications consideration:
  — If you plan to use SIP trunking, and you have a firewall set up, ensure that the ports you intend to use have been allowed.

"Using VoIP to tandem systems" on page 327, and "Configuring fallback over a VoIP MCDN network" in the *Device Configuration Guide* (NN40020-300).

Configuring VoIP trunk media parameters

The VoIP trunk media parameters allow you to specify the order in which the trunk will select IP telephony system controls for codecs, jitter buffers, silence suppression and payload size.

The following path indicates where to access the VoIP trunk media parameters in Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources > IP Trunks**

For details about the fields on this panel, refer to "H323 Media Parameters" on page 122 and "SIP Media Parameters" on page 126.

1. On the Modules panel, in the Module type column, select the IP Trunks line.
2. In the bottom panel, select the H323 or SIP Media Parameters tab.
3. Enter the information that supports your system. Ensure that these settings are consistent with the other systems on the network:
   - Preferred Codecs: Choose codecs in the same order for all remote equipment.
   - Settings:
     — Enable Voice Activity Detection: Disable or enable this feature, based on network requirements. Also refer to "Silence suppression" on page 529.
     — Jitter buffer - Voice: Either choose auto to let the system determine resource availability, or choose a buffer size.
     — Payload Size: Change the defaults to coordinate with other systems on the network.

Operations note: Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference:

— Locate fax machine away from other telephones.

— Turn the speaker volume on the fax machine to the lowest level, or off, if that option is available.

- Force G.711 for 3.1k audio - When enabled, the system forces the VoIP trunk to use the G.711 codec for 3.1k audio signals such as modem or TTY machines.

4 Set up the local gateway parameters. ("Setting up the local gateway" on page 383)

Setting up the local gateway

The call signaling method used by the local gateway defines how the BCM prefers call signaling information to be directed through VoIP trunks. Call signaling establishes and disconnects a call. You set this information in the local gateway panels.

If the network has a gatekeeper (H.323 trunks, only), the BCM can request a method for call signaling, this request is granted depending on the configuration of the gatekeeper. Ultimately, the gatekeeper decides which call signaling method to use. Refer to "VoIP interoperability: Gatekeeper configuration" on page 389.

The following path indicates where to access the local gateway in Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources > IP Trunks**.

1 In the bottom panel, select the **H323 Settings** or **SIP Settings** tab.

2 Choose the settings that you need for your system:

- Fallback to circuit-switched: define how you want the system to handle calls that the system fails to send over the VoIP trunk.

Note: Enabled-TDM enables fallback for calls originating on digital telephones. This is useful if your IP telephones are connected remotely, on the public side of the BCM network, because PSTN fallback is unlikely to result in better quality of service in that scenario.

- Forward redirected OLI - If the box is selected, the OLI of an internal telephone is forwarded over the VoIP trunk when a call is transferred to an external number over the private VoIP network. If the box is cleared, only the CLID of the transferred call is forwarded.
- Send name display - When selected, the telephone name is sent with outgoing calls to the network.
- Remote capability MWI - This setting must coordinate with the functionality of the remote system hosting the remote voice mail.
- Call Signaling: Determine how the calls are delivered over the network:
  - **Direct**: call signaling information is passed directly between endpoints.
    Note: You will need to set up remote gateways ("Setting up remote gateways" on page 385).
  - **Gatekeeper Resolved**: all call signaling occurs directly between H.323 endpoints. This means that the gatekeeper resolves the phone numbers into IP addresses, but the gatekeeper is not involved in call signaling.

— **Gatekeeper Routed**: uses a gatekeeper for call setup and control. In this method, call signaling is directed through the gatekeeper.

— **Gatekeeper Routed no RAS:** Use this setting for a NetCentrex gatekeeper. With this setting, the system routes all calls through the gatekeeper but does not use any of the gatekeeper Registration and Admission Services (RAS).

— Refer to "Using CS 1000 as a gatekeeper" on page 389 for specific information about configuring the gatekeeper for H.323 trunks.
Network note: If your private network contains a Meridian 1-IPT, you cannot use Radvision for a gatekeeper.

- Call signaling port: If there are VoIP applications that require non-standard call signaling ports, enter the port number here. 0 = the system uses the first available port.
- RAS port: If the VoIP application requires a non-standard RAS port, enter the port number here. 0 = the system uses the first available port.
- Enable H245 tunneling: Select or deselect the check box to allow or disallow H.245 messages within H.225. Note that the VoIP Gateway service must be restarted for any change to take effect.
- Gatekeeper Support: Fill out these fields if the network is controlled by a Gatekeeper: Also refer to "VoIP interoperability: Gatekeeper configuration" on page 389.
  — Primary Gatekeeper IP: This is the IP address of the primary gatekeeper.
  — Backup Gatekeepers: NetCentrex gatekeeper does not support RAS, therefore, any backup gatekeepers must be entered in this field. Gatekeepers that use RAS can provide a list of backup gatekeepers for the end point to use in the event of the primary gatekeeper failure.
- In the Alias names field, enter all the alias names required to direct call signals to your system.
- Gateway protocol - Select SL-1 for BCM 2.5 systems. Select CSE for BCM 3.0 and newer systems. Or select None.
- Registration TTLs: Specifies the KeepAlive interval
- Gateway TTLs: This protocol should match all other systems on the network.
- Status: This field displays the current status of the gatekeeper.

3 Suggested next steps:

- Ensure router settings, firewalls and system ports are set correctly to support IP traffic over the trunks.
- "Configuring lines" on page 129
- "Configuring lines: Target lines" on page 141
- "Setting up VoIP trunks for fallback" on page 391
- Ensure private network dialing plan and access settings matches the rest of the private network: "Dialing plan: Private network settings" on page 281
- Private networking: "Private networking: Basic parameters" on page 315
- Assigning the VoIP line pools to system telephones: "Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300).

Setting up remote gateways

The following explains how to set up your system to place calls through VoIP trunks. The system at the other end of the call must be set up to receive VoIP calls. For information about this, refer to "Configuring a remote gateway (H.323 trunks)" on page 385.

Configuration note: If the VoIP network has a gatekeeper, you do not need to configure remote gateways, as they are not used.

Configuring a remote gateway (H.323 trunks)

The following explains how to configure the BCM to communicate with other BCMs and/or other VoIP gateways such as Meridian IPT using H.323 trunks. The remote gateway list must contain an entry for every remote system to which you want to make VoIP call.

Gatekeeper note: If your system is controlled by a gatekeeper, you do not need to establish these gateways. Refer to "VoIP interoperability: Gatekeeper configuration" on page 389.

The following path indicates where to access the remote gateway in Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources**

1. On the Modules panel, in the **Module type** column, select IP Trunks.
2. In the bottom panel, select the **Routing Table**.
3. Click **Add**.
   The **Add Remote Gateway** dialog box appears.
4. Enter a Name and Destination Digits for the remote gateway.
5. Enter the appropriate information for the remote system:
   - Destination IP: Indicate the IP address of the device you want to connect with. This code will be part of your destination code programming.
   - GW Type: Choose the variable that identifies the type of system or application being connected to.
   - GW Protocol: Choose the protocol that supplies the required call features. None (default) supplies no feature. This setting is dictated by the type of remote system.
   - VoIP Protocol: Select signalling to endpoint - SIP or H.323.
   - QoS Monitor: Enable this feature if you are using fallback to PSTN lines and the network supports QoS monitoring.
   - Tx Threshold: Indicate the level of transmission at which the signal must be maintained. If the signal falls below this level the call falls back to PSTN.
6. Click **OK**.

Configuring VoIP lines

VoIP lines require a keycode to activate. You also need to set gateway parameters and system IP parameters to enable the trunks.

You must also set up target lines when you use these trunks.

The following path indicates where to set up target lines in Element Manager:

- Element Manager: **Configuration > Telephony > Lines > Target Lines**

Prerequisites

Complete the following prerequisites checklist before configuring the modules.

The gateway and IP network is set up correctly. Refer to the following procedures: • "Configuring VoIP trunk media parameters" on page 382 • "Setting up the local gateway" on page 383 • "Setting up remote gateways" on page 385 • "VoIP interoperability: Gatekeeper configuration" on page 389	
Obtain all relevant central office/service provider information for the type of trunk.	

Configuring VoIP line features

The following procedure describes the fields that need to be confirmed or set for these lines. For detailed field descriptions, refer to "Configuring lines" on page 129.

1 Confirm or change the settings on the Line/Trunk main panel:

- Line: Unique number
- Trunk type: VoIP
- Name: identify the line or line function
- Control Set: identify a DN if you are using this line with scheduling.
- Line Type: define how the line will be used. If you are using routing, ensure it is put into Bloc (A to F)
- Prime Set: If you want the line to be answered at another telephone if the line is not answered at the target telephone, otherwise, choose None.
- Pub. Received #: Not applicable
- Priv. Received #: Not applicable
- Distinct Ring: If you want this line to have a special ring, indicate a pattern (2, 3, 4, or None).

2 Configure the trunk/line data:

In the top panel ensure a loop trunk is selected. In the bottom panel, select the Preferences tab.

- Aux. ringer: If your system is equipped with an external ringer, you can enable this setting to allow this line to ring at the external ringer.

3 On the bottom panel, under the Restrictions tab:

- Use remote package: If this line is used for remote call-ins or is part of a private network, ensure you specify a valid remote package.

4 Set the restriction and remote restrictions scheduling (Restrictions tab):

- Line Restrictions: Enter a valid restriction filter for the Normal schedule, and any other schedules that you want this line to be part of. (outgoing calls)
- Remote Restrictions: Enter a valid remote access package for the Normal schedule, and any other schedules that you want this line to be part of. (incoming calls from remote users or private networks)

5 Suggested next steps:

- "Configuring lines: Target lines and DASS2" in the *Device Configuration Guide* (NN40020-300)
- Also refer to "Line Access - Line Pool Access tab" in the *Device Configuration Guide* (NN40020-300)
- "Dialing plan: Routing and destination codes" on page 259
- "Dialing plan: Private network settings" on page 281

Chapter 45
VoIP interoperability: Gatekeeper configuration

The following describes the use of a gatekeeper for your H.323 VoIP trunks.

Refer to the gatekeeper software documentation for information about changing IP addresses.

Gatekeeper notes:

- The BCM has been tested by Nortel to be compliant with CS 1000 gatekeeper applications.
- A gatekeeper may help to simplify IP configuration or the BCM dialing plan; however, it does not simplify the network dialing plan.

Using CS 1000 as a gatekeeper

Both the BCM and the CS 1000 must be set to the parameters described in the following information for the gatekeeper to work effectively. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for detailed information on configuring a CS 1000 gateway.

For CS 1000, the Network Routing Service (NRS) can be configured and maintained through a web interface called NRS Manager. NRS Manager replaces the CS 1000 GK admin tool.

Review the following information before attempting to use the CS 1000 as a gatekeeper:

- Before a Gateway Endpoint registers with the CS 1000 gatekeeper it must first be added to the gatekeeper configuration.
- Before a registered Gateway Endpoint makes calls, it must have its routing entry information assigned within the gatekeeper configuration.
- Before any of these configuration changes become part of the gatekeeper active configuration, they must be committed to the active database.

BCM requirements

Set the BCM Local Gateway IP interface to the following using BCM Element Manager (go to **Configuration > Resources > Telephony Resources > {Select IP Trunk} > H323 Settings tab**):

- Set **Call Signaling** to GatekeeperRouted or GatekeeperResolved.
- Set **Primary Gatekeeper IP** to the IP address of the NRS.
- Set **Alias Names** to the Alias name that was used when the H.323 Endpoint for the BCM was created on the NRS.

In order to make a BCM 3.01 (or later)-to-CS 1000 call, ensure that the BCM routes and dialing plan (used to reach the CS 1000 systems) match the numbering plan entry assigned to the CS 1000 systems through NRS Manager.

Similarly, to make a CS 1000 system-to-BCM 3.01 (or later) call, ensure that the numbering plan entry assigned to the BCM (through NRS Manager) matches the dialing plan information configured on the CS 1000 systems.

CS 1000 configuration

You must use NRS Manager to configure the CS 1000.

The NRS server must be enabled and properly configured before any NRS data can be provisioned using NRS Manager. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for detailed information on configuring a CS 1000 gateway.

Chapter 46
Setting up VoIP trunks for fallback

The following path indicates where to access setting VoIP trunks for fallback in the Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources > IP Trunks > H323 Settings tab**

Task: Configure VoIP trunks to allow fallback to PSTN lines

- "Configuring routes for fallback" on page 391
- "Example: A private network configured for fallback" on page 396

Configuring routes for fallback

Configuring routes allows you to set up access to the VoIP and the PSTN line pools. These routes can be assigned to destination codes. The destination codes then are configured into schedules, where the PSTN line is assigned to the Normal schedule and the VoIP route is assigned to a schedule that can be activated from a control set.

For details about route and schedule configuration, refer to the information under the headings below:

- "Adding routes for fallback" on page 392
- "Assigning the line pools to routes" on page 392
- "Adding the destination code for the fallback route" on page 393
- "Configuring the schedules for the destination codes" on page 394
- "Setting up the VoIP schedule to overflow" on page 395

Pre-configuration requirements

- If you have not already done so, remember to define a route for the local PSTN for your own system so users can still dial local PSTN numbers.

- Ensure the PSTN and VoIP line pools have been configured before you continue with this section. For information about creating a VoIP line pool, see "Configuring VoIP trunk gateways" on page 381. To configure PSTN lines, select **Configuration > Telephony > Lines > Active Physical Lines**.

Note: If you already have routes for your PSTN or VoIP line pools configured, you do not need to configure new routes, unless you cannot match the dialed digits.

Adding routes for fallback

Enter the routes you want to use for normal and fallback traffic.

To add routes, select **Configuration > Telephony > Dialing Plan > Routing**.

To add the PSTN route to other system

1. Type a number between 001 and 999.
   This route defines the PSTN route to the other system. Only numbers not otherwise assigned will be allowed by the system.
2. Click **OK**.

To add the PSTN route to the local PSTN lines

1. In the **Route** field, type a number between 001 and 999.
   This route defines the PSTN route to your local PSTN.
2. Click **Save**.

To add the VoIP route

1. In the **Route** field, type a number between 001 and 999.
   This route defines the VoIP route.
2. Click **Save**.

Assigning the line pools to routes

Assign the line pools to the routes you created in the previous section.

To assign PSTN line pool (to other system)

1. Click the route you created between the PSTN line and the other system.
2. In the **Use Pool** box, type the letter of the line pool for the PSTN lines to the other system.
3. In the **External Number** field:
   If this is a public PSTN line, enter the dial numbers that access the other system through the PSTN. For example: 1<area code><local code>.

4 In the **DN Type** box, choose **Public**.

To assign PSTN line pool to local PSTN lines

1 Click the route you created for your local PSTN line.

2 In the **Use Pool** box, type the letter of the line pool for the PSTN line.

3 In the **External Number** field: leave this field blank.

4 In the **DN Type** box, choose **Public**.

To assign VoIP line pool

1 Click the route you created for the VoIP lines.

2 In the **Use Pool** field, type the letter of the line pool for the VoIP lines.

3 Leave the **External Number** field blank unless the destination digit you are using for the remote gateway is different than the number you want to use for the destination code.

4 In the **DN Type** box, choose **Private**.

Go to the next section: "Adding the destination code for the fallback route" on page 393.

Adding the destination code for the fallback route

Create a destination code that includes the VoIP and PSTN routes that you created in "Adding routes for fallback" on page 392 to respond to the same access number (destination code). When this code is dialed, the BCM will select the VoIP line, if possible. If the line is not available, the call will fall back to the PSTN line.

As well, you need to create, or ensure, that your destination code 9 includes a Normal and VoIP schedule that includes the route you created to the local PSTN.

Note: If you already have a line pool access code defined as 9, you will need to delete this record before you create the destination code.

To create destination codes for your fallback route

1 Click **Configuration > Telephony > Dialing Plan > Routing > Destination Codes** tab.

2 Click **Add**.
The **Add Destination Code** dialog box appears.

3 Enter one or more digits for this destination code.

4 Click **OK** to close the dialog box.

Example:

Destination code digit: If it is available, you might want to use the same number that you used for the destination code of the gateway.
If you have multiple gateways, you could use a unique first number followed by the destination digits, to provide some consistency, such as 82, 83, 84, 85 to reach gateways with destinations digits of 2, 3, 4 and 5.
The number you choose will also depend on the type of dialing plan the network is using. Networks with CDP dialing plans have unique system codes. However, with networks using UDP, this is not always the case, therefore, you need to be careful with the routing to ensure that the codes you choose are unique to the route. This will also affect the number of digits that have to be added or absorbed. It is helpful to use the Programming Records to plan network routing so you can determine if there will be any conflicts with the destination codes you want to use.

Configuring the schedules for the destination codes

Under the destination code heading you created in the previous section, click the **Schedules** key, then choose the appropriate schedules:

To configure the VoIP schedule for all fallback destination codes

1. Change **First Route** to the route you configured for your VoIP line.
2. Set the **Absorbed length** to absorb the amount of the destination code that is not part of the dialout for the trunk.

Normal schedule for all fallback destination codes:

1. Change **Use Route** to the route you configured for your PSTN fallback line (the line to the other system).
2. Set the **Absorbed length** to absorb the amount of the destination code that is not part of the DN for the other system.

Examples:

Absorbed length, VoIP schedule: If the remote gateway destination digit is 2, which is part of the remote system DN structure (CDP network), and you specified a destination code of 82, set this field to 1, so that the 2 is still part of the dialout.

If the destination code is different from the remote gateway destination digits, and you entered an External # into the route record (the destination digit for the remote system), set the absorbed length to the number of digits in the destination code. The system will dial out the External # you entered in front of the rest of the number that the user dialed. This would occur if the network is set up with a UDP dialing plan.

Note: Do not add alternative routes (second or third). Since fallback is active, the system immediately falls back to the Normal schedule if the first route is not available.

Absorbed length, Normal schedule: If this is a private network PSTN line, and the network uses a CDP dialing plan, and the remote system identifier is 2, which is part of the remote system DN structure, and you specified destination digit of 2 for the remote gateway, then configured a destination code of 82, set this field to 1, so that the 2 is still part of the dialout.
If the destination code is different from the private access code/destination digits for the remote system (UDP dialing plan) or this is a public PSTN, enter private access code or the public access number to the remote system into the External # field on the route record. In this case, set the absorbed length to the number of digits in the destination code. The system will dial out the External # you entered in front of the rest of the number that the user dialed.

Setting up the VoIP schedule to overflow

Once you have configured the routing and destination codes, ensure that the Routing Service schedule allows fallback (Overflow) and allows you to activate the service from a control set. You will note that the Routing Service does not have a Normal schedule. This is because the Normal schedule is the schedule that runs when no routing services are active.

To set up the VoIP schedule for routing services

1. Double-click Sched 4 and rename it **VoIP** (**Configuration > Telephony > Scheduled Service > Schedule** Column).
2. Click **VoIP**.
   The VoIP schedule panel appears in the right frame.
3. Change the **Routing Svc** to **Manual**.
4. Select the **Overflow** check box.
5. Next steps:

   The following describes some further actions you may need to take to ensure that fallback is working:

   — “Activating the VoIP schedule for fallback” on page 395
   — “Deactivating the VoIP schedule” on page 396

Activating the VoIP schedule for fallback

Before activating the VoIP schedule, calls using the destination code are routed over the PSTN. This is because the system is set to use the Normal schedule, which routes the call over the PSTN. Once the VoIP schedule is activated, calls made with the VoIP destination code are routed over the VoIP trunk.

The VoIP line must be activated (**FEATURE 873**) from the control set for the VoIP trunk, which is specified when the trunk is created (**Configuration > Telephony > Lines > Active VoIP Lines**).

To activate the VoIP line from the control set

1. Dial **FEATURE 873** from the control set for the VoIP trunk.
   The phone prompts you for a password.
2. Type the password (default - admin: 23646).
3. Press OK.
   The first schedule appears.
4. Scroll down the list until VoIP is selected.
5. Press OK.
   The VoIP schedule stays active, even after a system reboot, and can only be manually deactivated.

Deactivating the VoIP schedule

To deactivate a schedule

1. Dial **FEATURE #873**. The phone prompts you for a password.
2. Type the password.
3. Press OK. The system returns to the Normal schedule.

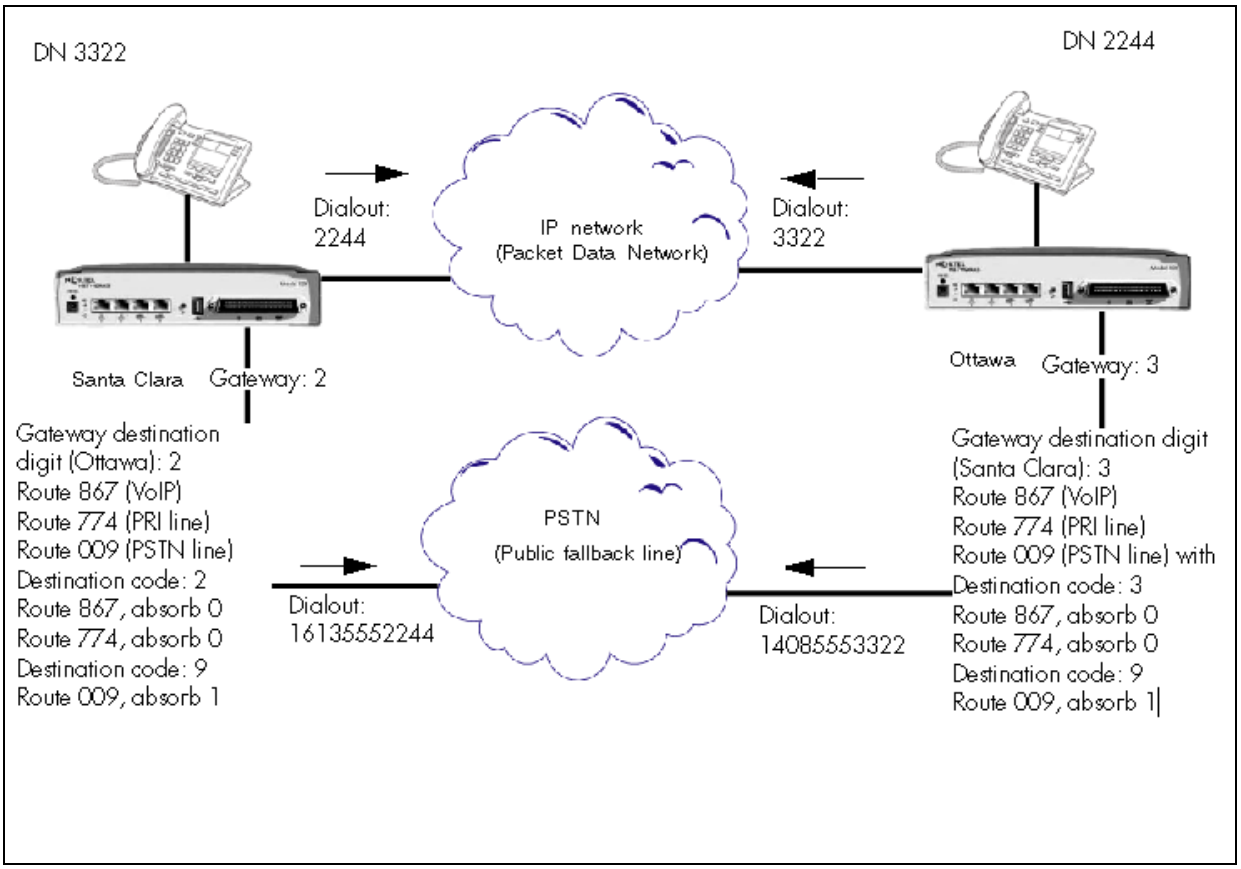
Example: A private network configured for fallback

The following describes a sample BCM configuration, which includes:

- "Activating the VoIP schedule for fallback" on page 395
- "Deactivating the VoIP schedule" on page 396

In this scenario, shown in Figure 117, two BCMs in different cities are connected through a WAN. One BCM is in Ottawa, the other is in Santa Clara. Both VoIP trunks and an PRI SL-1 line connect the system in a private network.

Figure 117 Example PSTN fallback



BCM Santa Clara	BCM Ottawa
• IP address: 47.62.84.1	• IP address: 47.62.54.1
• DNs 3000-3999	• DNs 2000-2999
• From this system, dial 9 to get onto PSTN	• From this system, dial 9 to get onto PSTN
• Dialing plan: CDP	• Dialing plan: CDP, destination code is part of DN

Routing	Routing
• Target DN 2244 (first digit is unique to system)	• Target DN 3322 (first digit is unique to system)
• Remote gateway destination digit: 2	• Remote gateway destination digit: 3
• Destination code: 2	• Destination code: 3
• VoIP/private network dialout: no external #, user dials 2244 (no absorbed digits)	• VoIP/private network dialout: no external #, user dials 3322 (no absorbed digits)

The systems already communicate through a PRI line, which will be configured to be used for fallback. Both systems already have all keycodes installed for eight VoIP lines, and resources properly allocated for VoIP trunking. For information about keycodes, see the *Keycode Installation Guide* (NN40010-301).

Each BCM has 10 telephones that will be using VoIP lines. In this setup, only eight calls can be sent or received over the VoIP trunks at one time. If all 10 telephones attempt to call at the same time, two of the calls will be rerouted to the PSTN or other alternate routes if multiple routing is set up in the destination code schedule.

System programming for networking and fallback routes

Table 81 provides the settings that are required for both systems to create a fallback network.

Table 81 Fallback configuration to create fallback between two systems (Sheet 1 of 2)

Task	Settings for Santa Clara	Settings for Ottawa	Location in Element Manager
Set up a Control set for each VoIP line	3321	2221	**Configuration > Telephony > Sets > All DNs**
Set first preferred Codec	G.729		**Configuration > Resources > Telephony Resources > IP Trunks**, H.323 Media Parameters tab.
Set voice activity detection	Selected		
Set Jitter Buffer	Medium		
Put 8 VoIP lines into the same line pool	BlocF		
Give all system telephones access to the VoIP line pool	BlocO		**Configuration > Telephony > Dialing Plan > Line Pools**
Confirm or assign target lines to all DNs or Hunt Groups t.	<targetline #>		**Configuration > Telephony > Lines >Target Lines**
Configure the target lines that you assigned.	Control set: 3321	Control set: 2221	**Configuration > Telephony > Lines > Target Lines** >Line XXX
	Trunk/Line data: Line Type: Private If busy: To prime		
	Prime set: DN 3321 Received number: 3322	Prime set: DN 2221 Received number: 2244	
Create remote gateway record for remote BCM	Destination IP: 47.62.54.1	Destination IP: 47.62.84.1	**Configuration > Resources >Telephony Resources > IP Trunks > Routing Table** **Destination digits note:** In this case, the systems use a Coordinated Dialing Plan (CDP) network, and the destination digit is included in the DN.
	QoS Monitor: Enabled Transmit Threshold: 3.5 (moderate quality) Gateway Type: BCM3.6 Gateway protocol: None		
	Destination Digits (Ottawa): 2	Destination Digits (Santa Clara): 3	

Table 81 Fallback configuration to create fallback between two systems (Sheet 2 of 2)

Task	Settings for Santa Clara	Settings for Ottawa	Location in Element Manager
Set up Scheduling to allow you to manually start and stop schedules.	Service setting: Manual Overflow: Selected		**Configuration > Telephony > Scheduled Services**, VoIP (Schedule 4).
Confirm or set up a route using the line pool to access the local PSTN.	Route: 009		**Configuration > Telephony > Dialing Plan > Routing**
	External #	External #	
	Line Pool: <publiclinepool> DN type: Public		
Set up a route that contains the PRI fallback lines.	Route: 774 Dialout: N/A PSTN Line Pool: BlocA DN type: Private		**Configuration > Telephony > Dialing Plan > Routing**
Set up a route that contains the VoIP line pool.	Route: 867 Dialout: N/A VoIP Line: BlocF DN type: Private		**Configuration >Telephony > Dialing Plan > Routing**
Create a destination code that matches the Destination Digit(s).	Destination code: 2	Destination code: 3	
Define the Normal and VoIP shedules.	Normal: Route 774, Absorb 0 digits VoIP: Route 867, Absorb 0 digits		**Configuration > Telephony > Scheduled Services**
Confirm or create a destination code for the PSTN. Define Normal and VoIP schedules.	Destination code: 9 Normal: Route 009, absorb All digits VoIP: Route 009, absorb All digits		
Activate the VoIP schedule from the control set.	3321	2221	FEATURE **873**

Making calls through a private VoIP network gateway

From a telephone on BCM Ottawa, a caller dialing to a telephone on BCM Santa Clara must dial the destination code, which includes the destination digits for the BCM Santa Clara remote gateway, and the DN of the telephone. For example, dialing 3322 would connect as follows:

- 3 is the destination code. If a suitable level of QoS is available, the call is routed through the VoIP trunks and through the remote gateway with a destination digit of 3. The call is sent across the PDN using the IP address of the Santa Clara BCM.
- 3322 is linked to the target line associated with DN 3322.
- The call arrives at the phone with the DN 3322.

If a user in Santa Clara wanted to make a local call in Ottawa, they would dial 29, followed by the local Ottawa number. The digit 2 accesses the remote gateway for the VoIP line. The digit 9 accesses an Ottawa outside line.

Chapter 47
T.38 fax

If you are using the T.38 fax protocol, it is assumed that you have already configured IP trunks and gateways, and that they are functional. For more information on configuring VoIP trunks see "Configuring lines" on page 129.

T.38 fax is a Fax over IP (FoIP) gateway protocol that allows standard (T.30 or Group3) fax machines to make calls over IP-based networks. The T.38 fax protocol functions transparently with standard fax machines because it emulates a normal T.30 fax connection. Each endpoint of the IP trunk becomes a T.38 gateway. To use FoIP, you must have two or four MS-PEC III cards installed in your MSC card. Both endpoints must support the T.38 fax protocol and have this feature enabled.

Enabling T.38 fax

Complete these procedures to enable the T.38 fax protocol.

To verify codecs in Element Manager

1. Click **Configuration > Telephony Resources**.
2. In the Telephony Resources panel, select the row for IP Trunks.
   The details panel appears.
3. Click the **H323 Media Parameters** or the **SIP Media Parameters** tab.
4. Verify that the preferred codec appears in the **Selected List** field.

5 Verify that the codecs are set at the default before performing T.38 sessions.

To enable a T.38 fax

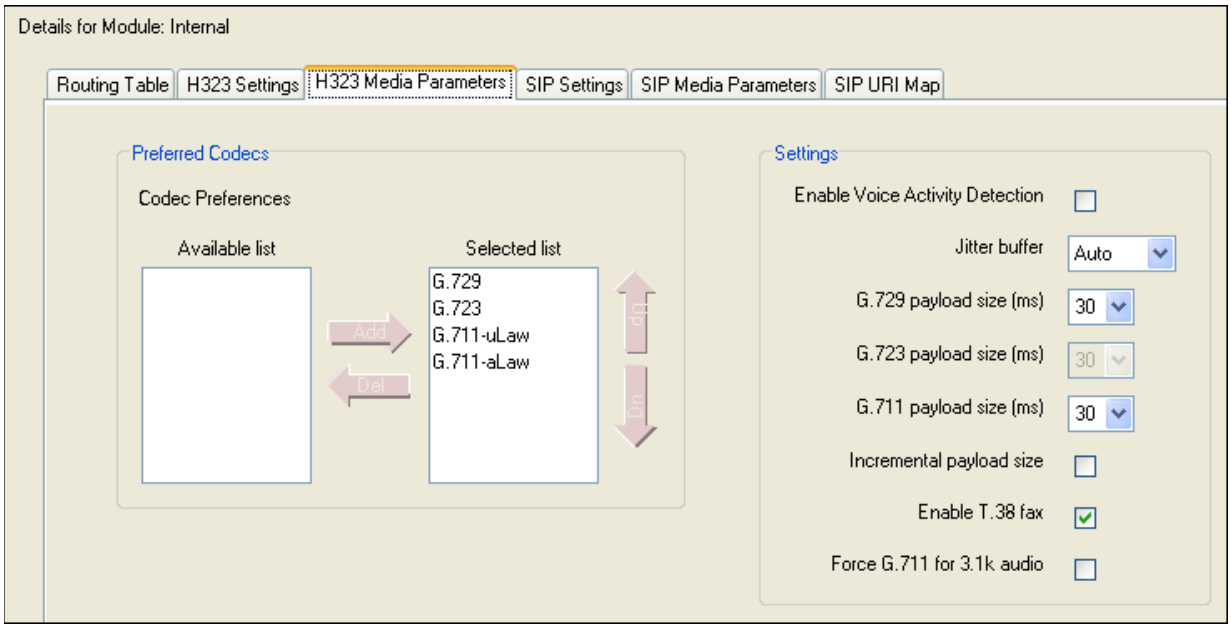
1 Click **Configuration > Telephony Resources**.

2 In the Telephony Resources panel, select the row for IP Trunks.
The details panel appears.

3 Click the **H323 Media Parameters** tab or the **SIP Media Parameters** tab.

4 Select the **Enable T.38 fax** check box.

Figure 118 H323 Media Parameters tab



Lines

To enable T.38 fax protocol you must configure the following:

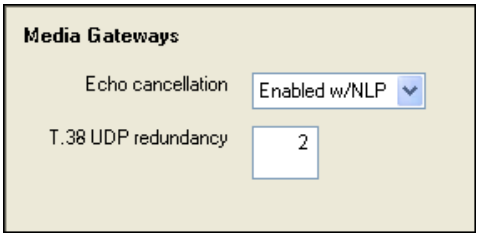
- Voice over IP (VoIP) lines (see "Configuring lines" on page 129)
- target lines (see "Configuring lines: Target lines" on page 141)
- call routing (see "Dialing plan: Routing configurations" on page 247)
- destination codes (see "Destination codes" on page 262)

Media gateways

T.38 UDP redundancy refers to the number of times IP packets (not fax pages) are sent, because TCP/UDP does not support packet validation (unlike TCP/IP).

To configure media gateways, click **Configuration > Resources > Media Gateways**.

Figure 119 Media Gateways panel



Note: For more details and instructions on how to configure media gateways, see "Media Gateways panel" on page 413.

T.38 Fax restrictions

Note: Fax tones that broadcast through a telephone speaker can disrupt calls on other telephones using VoIP trunks near the fax machine. Follow these suggestions to reduce the chance of your VoIP calls being dropped because of fax tone interference:

- Locate the fax machine away from other telephones.
- Turn the speaker volume on the fax machine to the lowest level, or off.

Note: Fax tones can be recorded in a voice mail box. In the rare event that fax tones are captured in a voice mail message, opening that message from a telephone using a VoIP trunk can cause the connection to fail.

Voice mail and T.38 FoIP share a maximum of eight fax ports. Voice mail supports only two fax ports.

If you allow fax messaging for the local VoIP gateway, you must be aware of the guidelines in "Operational notes and restrictions" on page 403 when you send and receive fax messages over VoIP trunks. For more information, see "VoIP trunk gateways" on page 367.

Operational notes and restrictions

Some fax machines cannot send faxes successfully over VoIP (T.38) trunks to the following destinations:

- CallPilot mailboxes
- CallPilot mailboxes accessed through auto-attendant
- Fax Transfer (calls transferred to a system fax device through the auto-attendant)

Use the following tips to avoid this problem:

- Avoid using manual dial on the originating fax machine. In some fax machines, dialing manually results in a much shorter call time-out.

- If you must dial manually, wait until the call is answered before you start the fax session.
- For Mailbox Call Answering only, if you must dial manually, enter the digit 8 as soon as you hear the mailbox greeting. This ensures that CallPilot initiates the fax session before the fax machine timer starts.

Note: Enter the digit 8 for Norstar Voice Mail User Interface (NVMUI) only. To enable fax call answering when using CallPilot User Interface (CPUI), enter 707.

- Increase the call duration by adding a timed pause to the end of the dialing string. This addition allows the call to ring at the destination before the fax machine call-duration timer starts. Refer to your fax machine documentation for more information on how to insert pauses into dial strings.
- Because the problem is related to the delay in initiating the fax session, reduce the number of rings for fax mailboxes Call Forward No Answer (CFNA).

Chapter 48
Port ranges overview

The Port Ranges panel provides a list of which Ports are currently being used for RTP/UDP, UDP, and Signaling. In the case of RTP over UDP and UDP, it allows changes to the ports being used.

For information on configuring port ranges, see "Port Ranges panel" on page 407.

Warning: Port configuration should not be changed unless absolutely necessary, such as in instances where port configurations are causing conflicts, or if a firewall is restricting communications over certain ports.

RTP over UDP

RTP over UDP is used by IP sets to connect to media gateways, and by IP trunks to connect to remote devices or PDM devices. All of these services require RTP over UDP. Each media gateway uses two ports. By default, RTP over UDP is set to use the port range 28000 - 28255. It's recommended that you keep 256 ports configured for RTP over UDP. The BCM requires a minimum of 110 ports to support necessary services. This includes 32 IP sets, 11 voice mail and contact center voiceports, and 12 trunks. Each of these devices requires two RTP over UDP ports.

You can configure up to ten separate ranges of ports.

UDP

UDP is used for T.38 Fax over UDP. By default, it uses the Range 20000 to 20255. You can configure up to ten separate ranges of ports. While the system can function with 12 ports, it is recommended that 256 ports are reserved.

Signaling Ports

Signaling ports are used by the system and cannot be modified. They are provided to show where conflicts with UDP or RTP occur.

Chapter 49
Port Ranges panel

The Port Ranges panel allows you to reserve ports for use by UDP (User Datagram Protocol). The Port Ranges panel consists of three tables: RDP over UDP, UDP, and Signaling.

Panel tabs	Tasks	Features
"RTP over UDP Port Ranges" on page 407	"Adding new RTP over UDP Port Ranges" on page 408	
"UDP Port Ranges" on page 409	"Deleting RTP over UDP Port Ranges" on page 408	
"Signaling Port Ranges" on page 410	"Modifying RTP over UDP Port Ranges" on page 409	
	"Adding new UDP Port Ranges" on page 409	
	"Deleting UDP Port Ranges" on page 409	
	"Modifying UDP Port Ranges" on page 410	

Warning: Do not change the ports unless necessary. If you do change the ports, make sure you review the minimum requirements for each protocol. As well, make sure that you configure your firewall to reflect any changes you make to the ports.

RTP over UDP Port Ranges

RTP (Real-time Transfer Protocol) over UDP ports are necessary for IP trunk traffic, such as for the transmission of audio and video signals across the Internet. These values should only be changed if you are interoperating with an unsupported product. The RTP over UDP table has two settings.

Figure 120 illustrates the Port Ranges panel.

Figure 120 Port Ranges panel

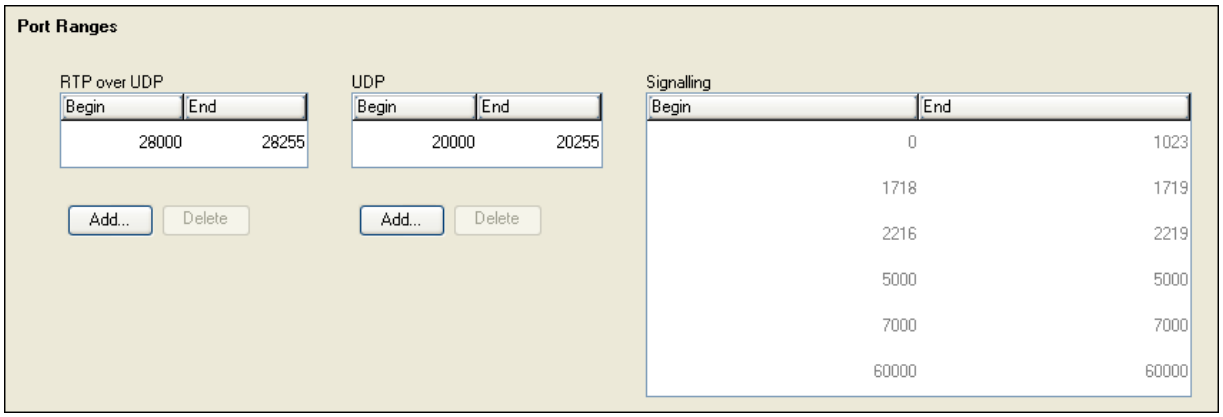


Table 82 RTP over UDP

Attribute	Value	Description
Begin	<numeric string>	The first port in the port range.
End	<numeric string>	The last port in the port range.

Adding new RTP over UDP Port Ranges

You can add up to ten port ranges.

To add new port ranges in the RTP over UDP table

1. On the RTP over UDP table, click **Add**.
   The Add RTP Port Range dialog appears.
2. In the **Begin** field, type the first port in the range.
3. In the **End** field, type the last port in the range.
4. Click **OK**.
   The new RTP port range appears in the table.

Deleting RTP over UDP Port Ranges

You cannot delete all port ranges from the table. You must keep at least one port range at all times.

To delete port ranges from the RTP over UDP table

1. On the RTP over UDP table, select the range to delete by clicking the appropriate row in either column.
2. Click **Delete**.
   The range disappears from the table.

Modifying RTP over UDP Port Ranges

To modify an entry on the RTP over UDP table

1 On the RTP over UDP table, select the entry to modify.

2 Type the new value.

UDP Port Ranges

UDP (User Datagram Protocol) ports are necessary for certain types of network communications. The UDP table has two settings, as shown in Table 83.

Table 83 UDP

Attribute	Value	Description
Begin	<numeric string>	The first port in the port range.
End	<numeric string>	The last port in the port range.

Adding new UDP Port Ranges

You can add up to ten port ranges.

To add new port ranges in the UDP table

1 On the UDP table, click **Add**.
The Add UDP Port Range dialog appears.

2 In the **Begin** field, type the first port in the range.

3 In the **End** field, type the last port in the range.

4 Click **OK**.
The new RTP port range appears in the table.

Deleting UDP Port Ranges

You cannot delete all port ranges from the table. You must keep at least one port range at all times.

To delete port ranges from the RTP over UDP table

1 On the UDP table, select the range to delete by clicking the appropriate row in either column.

2 Click **Delete**.
The range disappears from the table.

Modifying UDP Port Ranges

To modify an entry on the UDP table

1 On the UDP table, select the entry to modify.

2 Type the new value.

Signaling Port Ranges

Table 84 displays port ranges used for signaling. These port ranges cannot be modified. The Signaling Port Ranges table consists of two fields:

Table 84 Signaling

Attribute	Value	Description
Begin	<read-only numeric string>	The first port in the port range.
End	<read-only numeric string>	The last port in the port range.

Chapter 50
Media gateways overview

Certain types of IP communications pass through Media Gateways on the BCM. You can control the performance of these communications by adjusting the parameters for echo-cancellation and UDP Redundancy.

For detailed information on configuring the Media Gateways, see “Media Gateways panel” on page 413.

Chapter 51
Media Gateways panel

The Media Gateways panel allows you to set basic parameters that control IP telephony. The Media Gateways panel contains only two fields:

Figure 121 Media Gateways panel

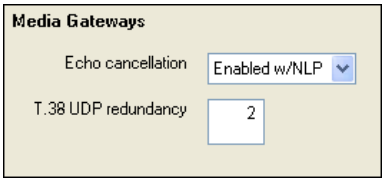


Table 85 General Settings

Attribute	Value	Description
Echo Cancellation	<drop-down menu> Enabled w/NLP Enabled Disabled	Enable or disable echo cancellation for your system. Default: Enabled w/NLP (check with your internet system administrator before changing this) **Echo Cancellation** selects what type of echo cancellation is used on calls that go through a Media Gateway. NLP refers to Non-Linear Processing.
T.38 UDP Redundancy	<numeric character string>	If T.38 fax is enabled on the system, this setting defines how many times the message is resent during a transmission, to avoid errors caused by lost T.38 messages.

Chapter 52
Call security and remote access

System restrictions are required to ensure that your system is used appropriately and not vulnerable to unauthorized use.

Call security includes:

- restriction filters, which limit outbound call access
- remote access packages, which limit system call feature access for users calling in over the Private or Public network
- Class of Service codes, which require remote system users to enter a password before they can access the system. CoS passwords also can have restriction filters applied.

Refer to the following topics:

- "Defining restriction filters" on page 415
- "Remote call-in programming" on page 419
  - "Creating Direct Inward System Access (DISA)" on page 420
  - "Defining remote access packages" on page 422
  - "Defining CoS passwords" on page 423

Call security works in conjunction with your dialing plan. Refer to "Dialing plans" on page 217.

Defining restriction filters

Restriction filters allow you to restrict the numbers that can be dialed on any external line within BCM. Up to 100 restriction filters can be created for the system.

To restrict dialing within the system, you can apply restriction filters to:

- outgoing external lines (as line restrictions)
- telephones (as set restrictions)
- external lines on specific telephones (as line/set restrictions)

Restriction filters can also be specified in Restrictions service for times when the system is operating according to a schedule. Dialed digits must pass both the line restrictions and the set restrictions. The line per set (line/set) restriction overrides the line restriction and set restriction.

Notes about restriction filters

A restriction filter is a group of restrictions and overrides that specify the external numbers or feature codes that cannot be dialed from a telephone or on a line. The restriction filters setting allows you to assign restrictions in one step as a single package of dialing sequences that are not permitted.

In addition to restricting telephone numbers, you can prevent people from entering dialing sequences used by the central office (the public network) to deliver special services and features. Some of these features provide the caller with dial tone after they have entered the special code (which often uses # or *), therefore, users have an opportunity to bypass restrictions. To prevent this from happening, you can create filters that block these special codes.

You create a filter by defining the dialing sequences that are denied. There are also variations of each sequence that you want users to be able to dial, these are called overrides. Overrides are defined within each restriction package for each filter.

Once you create the filters, you can assign the restrictions to a telephone, to a line, to a particular line on a telephone, and to remote callers.

Note: Filter 00 cannot be changed. Filter 01 has a set of defaults. Filters 02 to 99 can be set to suit your special requirements. See "Default filters (North America)" on page 417.

- Each programmable filter can have up to 48 restrictions.
- There is no limit on the number of overrides that can be allocated to a restriction. However, there is a maximum total of 400 restrictions and overrides allocated to the 100 programmable filters.
- The maximum length of a restriction is 15 digits.
- The maximum length of an override is 16 digits.
- Entering the letter *A* in a dialing sequence indicates a wild card, and represents any digit from 0 to 9.
- You can use * and # in a sequence of numbers in either a restriction or an override. These characters are often used as part of feature codes for other systems or for features provided by the central office (the public network).
- When restricting the dialing of a central office feature code, do not forget to create separate restrictions for the codes used for DTMF and pulse lines (for example, *67 and 1167).
- Do not string together a central office feature code and a dialing sequence that you want to restrict. Create a separate restriction for each.
- You can copy restrictions and overrides from one filter to another. You can use a restriction or override in any number of filters. Each time you use a restriction or override, it counts as one entry. For example, if restriction 411 exists in filters 01, 02 and 03, it uses up three entries of the 400 entries available.

- Removing a restriction from a filter has no effect on the contents of other filters, even if the restriction was copied to them.
- You cannot delete a filter. Removing the restrictions programmed on a filter makes it an unrestricted filter but the filter itself is not removed.

Default filters (North America)

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with 10 restrictions and some associated overrides. In Filter 01, Restriction 02 and Override 001 allow long distance toll free calls.

The dialing string 911, which is the number for emergency assistance in North America, is included as both a restriction and an override in Filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Table 86 Default restriction filters

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
01	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Note: Default filters are loaded when the system is initialized. A cold start restores the default filters.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are the default filters in these programming headings:

Table 87 Default filters for program headings

Filter	Heading	Sub-heading
02	System DNs	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Default filters (other)

Two profiles have global overrides which do not appear in Element Manager restriction programming and cannot be changed.

Australia: 000, 13144A

UK: 999, 112

Restriction filter examples

Line and set restrictions are shown in Figure 122 and Figure 123.

In Figure 122, a caller using line 001 could only dial long-distance numbers to area codes 212 and 718. A caller using line 003 could not dial any long-distance numbers. A caller using line 005 could dial long-distance numbers to area codes 212, 718, and 415.

Tips: To restrict dialing from outside the system (once a caller gains remote access), apply restriction filters to incoming external lines (as remote restrictions).

Figure 122 Line restriction example

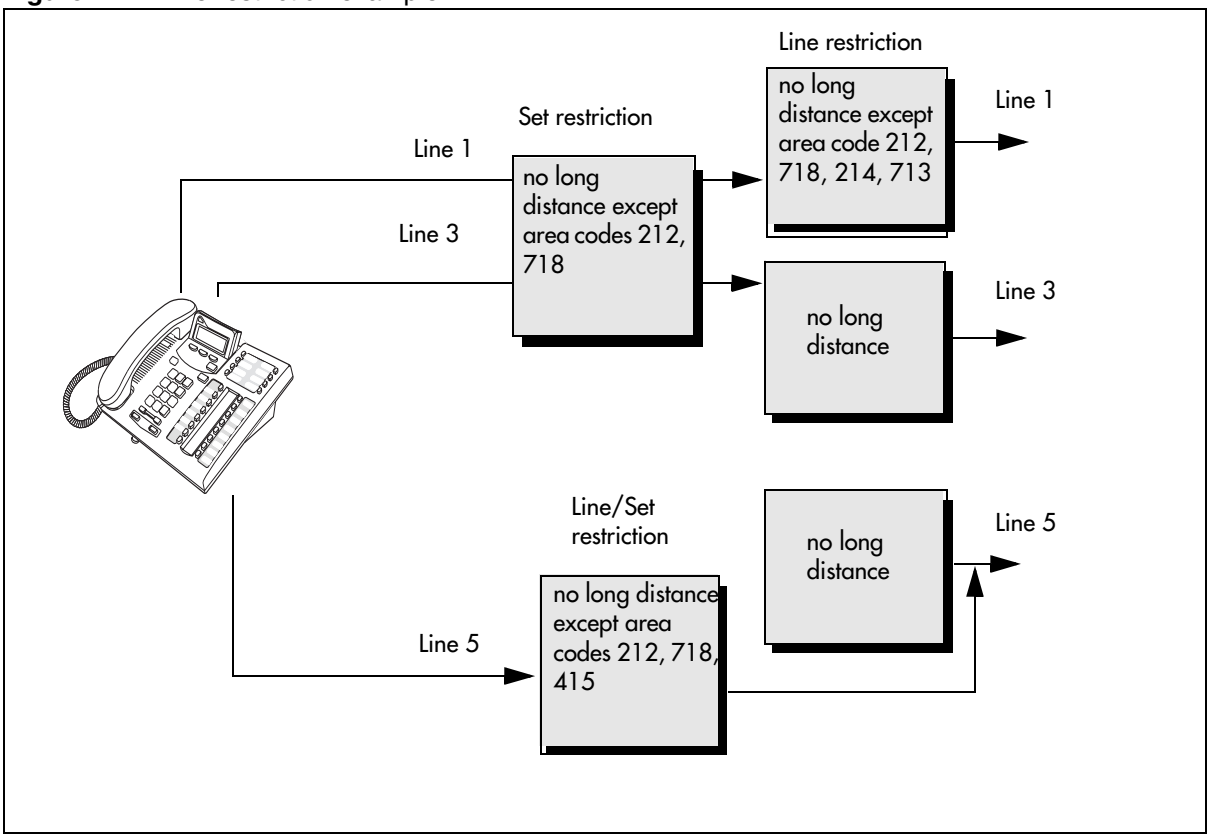
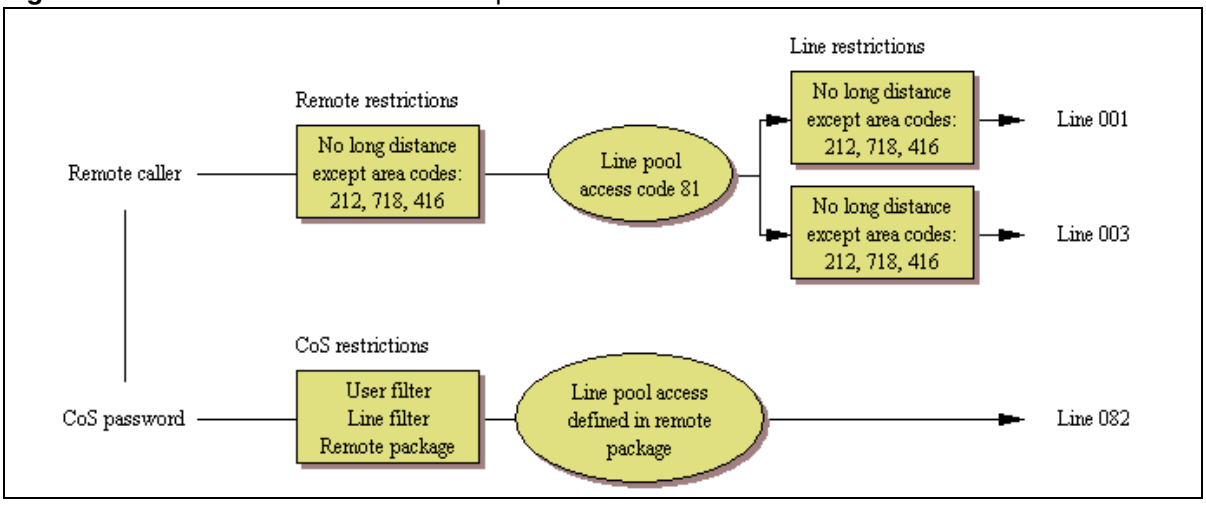


Figure 123, dialed digits must pass both the remote restriction and the line restriction. A remote caller can override these filters by dialing the DISA DN and entering a CoS password.

Figure 123 Remote line restriction example



Remote call-in programming

There are three aspects to remote call ins:

- Setting up lines to allow users access to the system ("Creating Direct Inward System Access (DISA)" on page 420.
- Setting up Remote Access Packages that determine what services the remote users can access.
- Setting up CoS passwords for users calling in through the PSTN on lines programmed with DISA. ("Defining CoS passwords" on page 423)

Creating Direct Inward System Access (DISA)

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a CoS password that determines what they are allowed to do in the system.

- Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default.
- T1 DID trunks: You cannot configure T1 DID trunks to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.
- You cannot program a DISA DN or Auto DN to VoIP trunks, because they act as auto-answer lines for private networks. However, you still need to assign remote access packages to the VoIP trunks, to ensure that remote access restrictions are properly applied to incoming calls trying to access the system or the system network.

Also refer to the following information:

- "Remote access line settings"
- "Remote access on loop start trunks" on page 421
- "Remote access on T1 DID and PRI trunks" on page 421
- "Remote access on DPNSS lines" on page 421
- "Remote access on a private network" on page 422

Remote access line settings

The remote access feature allows callers elsewhere on the private or the public network to access your BCM by dialing directly and not going through the attendant. After the remote user is in the system, they can use some of the system resources. You must enable remote access in programming before callers can use it.

BCM supports remote system access on a number of trunk types which may require the remote caller to enter a password for DISA.

The system resources, such as dialing capabilities, line pool access and feature access, that a remote user may access depends on the CoS password assigned to them. See "Defining CoS passwords" on page 423.

Note: Callers remotely access the BCM remote features setting by pressing * and the appropriate page code. See the *Device Configuration Guide* (NN40020-300) for a list of feature codes.

Remote access on loop start trunks

Loop start trunks provide remote access to BCM from the public network. They must be configured to be auto-answer to provide remote system access.

A loop start trunk **must** have disconnect supervision if it is to operate in the auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer without DISA, the system answers with system dial tone and no CoS password is required. In this case, the remote access package assigned to the line controls system capabilities.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a CoS password that determines which system capabilities are available to the caller.

Remote access on T1 DID and PRI trunks

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are:

- A remote caller is on the public network dialing standard local or long distance telephone numbers.
- DISA cannot be administered to a T1 DID and PRI trunk. You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN. If you program the dialed digits to the DISA DN, only the incoming calls that match the programmed DN will receive a DISA dial tone. Incoming calls with other digits will route to a target line.

Remote access on DPNSS lines

A remote caller can access a BCM system dial tone, select a line pool that contains exchange lines or DPNSS lines, then dial a number. The procedure is identical to dialing an outside number from an extension in the local system. The main features are:

- Calls coming from another switch to the BCM system are routed in two ways, depending on the Answer mode that you program. If the **Answer mode** is set to **Manual**, and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If **Answer mode** is set to **Auto**, BCM automatically answers the incoming call. Because most other DPNSS features are extension-specific, Nortel recommends that all DPNSS lines are configured as auto-answer lines.
- The Page feature is available to both remote callers and callers within the system. A remote caller must have DTMF capability to access the Page feature.
- The line redirection feature allows the originating party to redirect a call that is waiting a connection or re-connection to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Remote access on a private network

Systems connected to the private network deliver the last dialed digits to the destination BCM system for interpretation. The destination BCM system matches the digits to a target line or interprets the digits as a remote feature request. BCM then routes the call to the specified target line or activates the remote feature.

- By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are **not** answered with DISA. If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a CoS password.
- The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in "Understanding access codes" on page 229.
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN on the other system.
- Answer with DISA cannot be administer to voice over IP (VoIP), since they do not connect systems outside the private network. However, a user calling in remotely on another system on the network can use the trunk to access the system or a user calling in on a PSTN line can use the trunk to access the private network. To provide control for this type of access, ensure that you specify remote access packages for the trunk.

Defining remote access packages

The Remote access packages setting allows you to control the remote access to line pools and remote page.

Create a remote access package by defining the system line pools remote users can access. You then assign the package to individual lines, and to a particular Class of Service password (see "Defining CoS passwords" on page 423).

Defining CoS passwords

CoS passwords permit controlled access to the system resources by both internal and remote users.

- When an internal user enters a CoS password at a telephone, the restriction filters associated with the CoS password apply instead of the normal restriction filters.
- Similarly, when a remote user enters a CoS password on an incoming auto-answer line, the restriction filters and remote package associated with their CoS password apply instead of the normal restriction filters and remote package.

Notes about CoS passwords

The CoS password can define the set of line pools that may be accessed and whether or not the user has access to the paging feature.

The class of service (CoS) that applies to an incoming remote access call is determined by:

- the filters that you apply to the incoming trunk
- the CoS password that the caller used to gain access to BCM.
- in cases where DISA is not automatically applied to incoming calls, the remote caller can change the class of service by dialing the DISA DN and entering a CoS password.

Remote users can access system lines, line pools, the Page feature, and remote administration. The exact facilities available to you through remote access vary depending on how your installer set up your system.

Note: If the loop start line used for remote access is not supervised, auto-answer does not function and the caller hears ringing instead of a stuttered tone or the system dial tone.

Security Note:
CoS password security and capacity

- Determine the CoS passwords for a system randomly and change them on a regular basis.
- Users should memorize their CoS passwords and keep them private. Typically, each user has a separate password. However, several users can share a password or one user can have several passwords.
- Delete individual CoS passwords or change group passwords when employees leave the company.
- A system can have a maximum of 100 six-digit CoS passwords (00 to 99).

To maintain the security of your system, the following practices are recommended:

- Warn a person to whom you give the remote access number to keep the number confidential.
- Change CoS passwords often.
- Warn a person to whom you give a CoS password, to memorize the password and not to write it down.
- Delete the CoS password of a person who leaves your company.

Security Note: Remote users can make long distance calls.
Remember that a remote user can make long distance calls that are charged to your company. They can also access line pools and make page announcements in your office.

External access tones

You can hear some of the following tones when accessing BCM from remote location. Table 88 shows the different types of tones and what they mean.

Table 88 External access tones

Tone	What it means
System dial tone	You can use the system without entering a CoS password.
Stuttered dial tone	Enter your CoS password.
Busy tone	You have dialed a busy line pool access code. You hear system dial tone again after five seconds.
Fast busy tone	You have done one of the following: • Entered an incorrect CoS password. Your call disconnects after five seconds. • Taken too long while entering a CoS password. Your call disconnects after five seconds. • Tried to use a line pool or feature not permitted by your Class of Service. You hear system dial tone again after five seconds. • Dialed a number in the system which does not exist. Your call disconnects after five seconds.
	IP trunk lines do not produce tones when accessed from a remote location.

Chapter 53
Call Security: Configuring Direct Inward System Access (DISA)

This following describes the telephony configuration that allows users to call from a remote site into the system to access system features.

The following paths indicate where to access DISA settings in Element Manager and through Telset Administration:

- Element Manager:
  - **Configuration > Resources > Telephony Resources**
  - **Configuration > Telephony > Dialing Plan > Public Network**
  - **Configuration > Telephony > Dialing Plan > Private Network**
- Telset interface: ****CONFIG > System prgrming > Access codes**

Task: Configuring DISA DNs, Auto DNs, Answering with DISA
• Set up the system parameters for system users to call into the from a remote location. Note that Remote Access Packages are required for private network trunks, as well.

Refer to the following:

- "Remote access overview" on page 427
- "Setting up remote access on lines" on page 430

Remote access overview

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a CoS password that determines what they are allowed to do in the system.

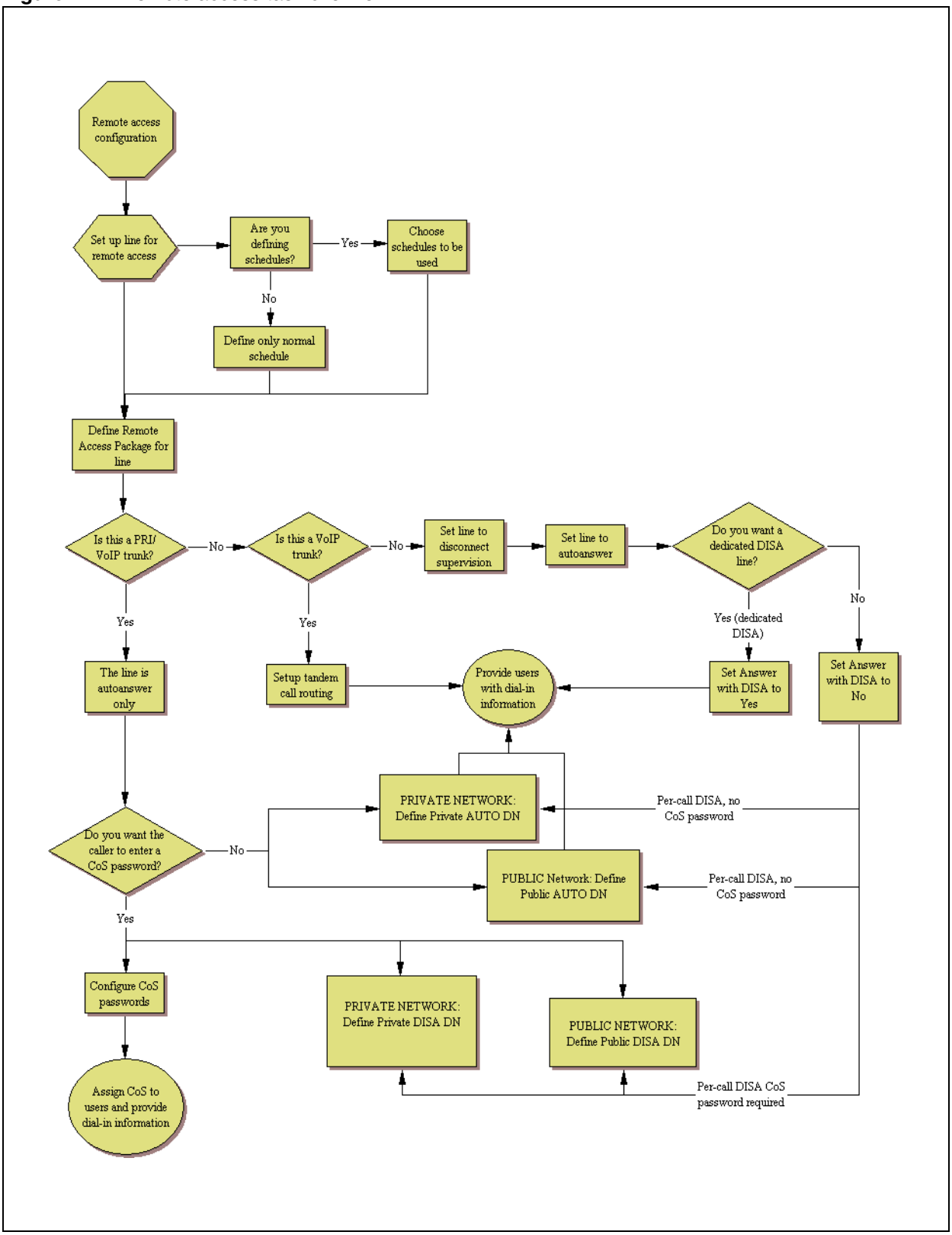
- Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default.
- T1 DID trunks: You cannot configure T1 DID trunks to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.

- You cannot program a DISA DN or Auto DN to VoIP trunks, because they act as auto-answer lines for private networks. However, you still need to assign remote access packages to the VoIP trunks, to ensure that remote access restrictions are properly applied to incoming calls trying to access the system or the system network.

For specific line programming, refer to "Setting up remote access on lines" on page 430.

Figure 124 provides an overview of the remote access configuration process.

Figure 124 Remote access task overview


Remote access configuration
Set up line for remote access
Are you defining schedules?
Yes
Choose schedules to be used
No
Define only normal schedule
Define Remote Access Package for line
Is this a PRI/ VoIP trunk?
No
Is this a VoIP trunk?
No
Set line to disconnect supervision
Set line to autoanswer
Do you want a dedicated DISA line?
Yes
Yes (dedicated DISA)
No
The line is autoanswer only
Setup tandem call routing
Provide users with dial-in information
Set Answer with DISA to Yes
Set Answer with DISA to No
PRIVATE NETWORK: Define Private AUTO DN
Per-call DISA, no CoS password
Do you want the caller to enter a CoS password?
No
PUBLIC Network: Define Public AUTO DN
Per-call DISA, no CoS password
Yes
Configure CoS passwords
PRIVATE NETWORK: Define Private DISA DN
PUBLIC NETWORK: Define Public DISA DN
Assign CoS to users and provide dial-in information
Per-call DISA CoS password required

Setting up remote access on lines

Setting up remote access on different types of trunks requires you to understand the trunk properties and how you want the system to answer the dial-in calls.

Refer to the following information:

- "Remote access on loop-start trunks" on page 430
- "Remote access on T1 DID trunks" on page 430
- "Remote access on PRI" on page 431
- "Remote access on DPNSS lines" on page 431
- "Remote access on a private network" on page 432
- "Other programming:" on page 432

Remote access on loop-start trunks

Loop-start trunks provide remote access to BCM from the public network. The trunks must be configured to be auto-answer to provide remote system access. Refer to "Configuring lines: T1-Loop start" on page 157.

A loop start trunk **must** have disconnect supervision if it is to operate in the auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer without DISA, the system answers with system dial tone and no CoS password is required. In this case, the restriction filters assigned to the line control system capabilities available to the caller.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a CoS password that determines which system capabilities are available to the caller.

Remote access on T1 DID trunks

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network.

The main differences are:

- A remote caller is on the public network dialing standard local or long distance telephone numbers.
- The digits received are delivered by the central office.
- DISA cannot be administered to a T1 DID trunk. You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN. If you program the dialed digits to the DISA DN, only the incoming calls that match the programmed DN will receive a DISA dial tone. Incoming calls with other digits will route to a target line.

Refer to "Configuring lines: T1-E&M" on page 151, "Configuring lines: T1-DID" on page 169.

Remote access on PRI

Remote system access on PRI trunks is similar to that of T1 E&M trunks connected to a private network.

The main differences are:

- A remote caller is on the public network dialing standard local or long-distance telephone numbers.
- The digits received are delivered by the central office.
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN.
- North America: Use incoming Call-by-Call (CbC) Service routing to map the call type to the DISA DN.

  With FX, INWATS, 900, and SDS service types, either a Service Id (SID) or a CDN is mapped to Target Line Receive Digits. This is programmed under "Configuring PRI Call-by-Call services" on page 148. DISA may be accessed by having the SID or CDN map to the DISA DN. This example has a Receive Digit Length = 4, DISA DN = 1234, and CbC Routing with (Service Type = FX, Map from SID = 2, Map to digits = 1234).

  A call presented to the BCM system with service type FX and SID 2 will be handled as follows:

  — The ISDN setup message will specify FX with SID = 2
  — The FX SID = 2 will be mapped to DISA DN digits 1234
  — The call will be answered with DISA.

Refer to "Configuring lines: PRI" on page 145.

Remote access on DPNSS lines

A remote caller can access a BCM system dial tone, select a line pool that contains exchange lines or DPNSS lines, and then dial a number. The procedure is identical to dialing an outside number from an extension in the local system. The main features are:

- Calls coming from another switch to the BCM system are routed in two ways, depending on the Answer mode that you program. If the **Answer mode** is set to **Manual**, and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If **Answer mode** is set to **Auto**, BCM automatically answers the incoming call. Because most other DPNSS features are extension-specific, Nortel recommends that you configure all DPNSS lines as auto-answer lines.
- The Page feature is available to both remote callers and callers within the system. A remote caller must have DTMF capability to access the Page feature.

- The line redirection feature allows the originating party to redirect a call that is waiting a connection or re-connection to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Refer to "Private networking: DPNSS network services (UK only)" on page 331.

Remote access on a private network

Systems connected to the private network deliver the last dialed digits to the destination BCM system for interpretation. The destination BCM system matches the digits to a target line or interprets the digits as a remote feature request. BCM then routes the call to the specified target line or activates the remote feature.

- By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are **not** answered with DISA. If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a CoS password.
- The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in "Dialing plan: Private network settings" on page 281.
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN on the other system.
- Answer with DISA cannot be administer to voice over IP (VoIP), since they do not connect systems outside the private network. However, a user calling in remotely on another system on the network can use the trunk to access the system or a user calling in on a PSTN line can use the trunk to access the private network. To provide control for this type of access, ensure that you specify remote access packages for the trunk. This type of call is called a tandem call.

Other programming:

- "Call security: Remote access packages" on page 439
- "Configuring CoS passwords for remote access" on page 443

Chapter 54
Call security: Restriction filters

The following describes the panels that are used to enter restriction filters and restriction overrides. You can have a maximum of 100 restriction filters on the system.

The following paths indicate where to access restriction filter settings in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Call Security > Restriction Filters**
- Telset Interface: ****CONFIG>Terminals and Sets, or **CONFIG>Lines**

Click one of the following links to connect with the type of information you want to view:

Panels	Tasks	Feature notes
"Restriction filters" on page 433	"Adding a restriction filter and exceptions" on page 435	"Default filters" on page 436
Using restriction filters:	"Restrictions (Line and Remote)" on page 137	
	"Class of Service table" on page 443	
	"Configuring scheduled service" in the *Device Configuration Guide* (NN40020-300)	
	"Hospitality - General" in the *Device Configuration Guide* (NN40020-300)	

Click the navigation tree heading to access general information about restriction filters.

Restriction filters

Restrictions are used to restrict outbound dialing. For example, restrictions can be applied to restrict dialing 1-900 numbers.

The restriction filters panel contains three list boxes. You progress from left to right as you populate the information.

Figure 125 Restriction Filters panels

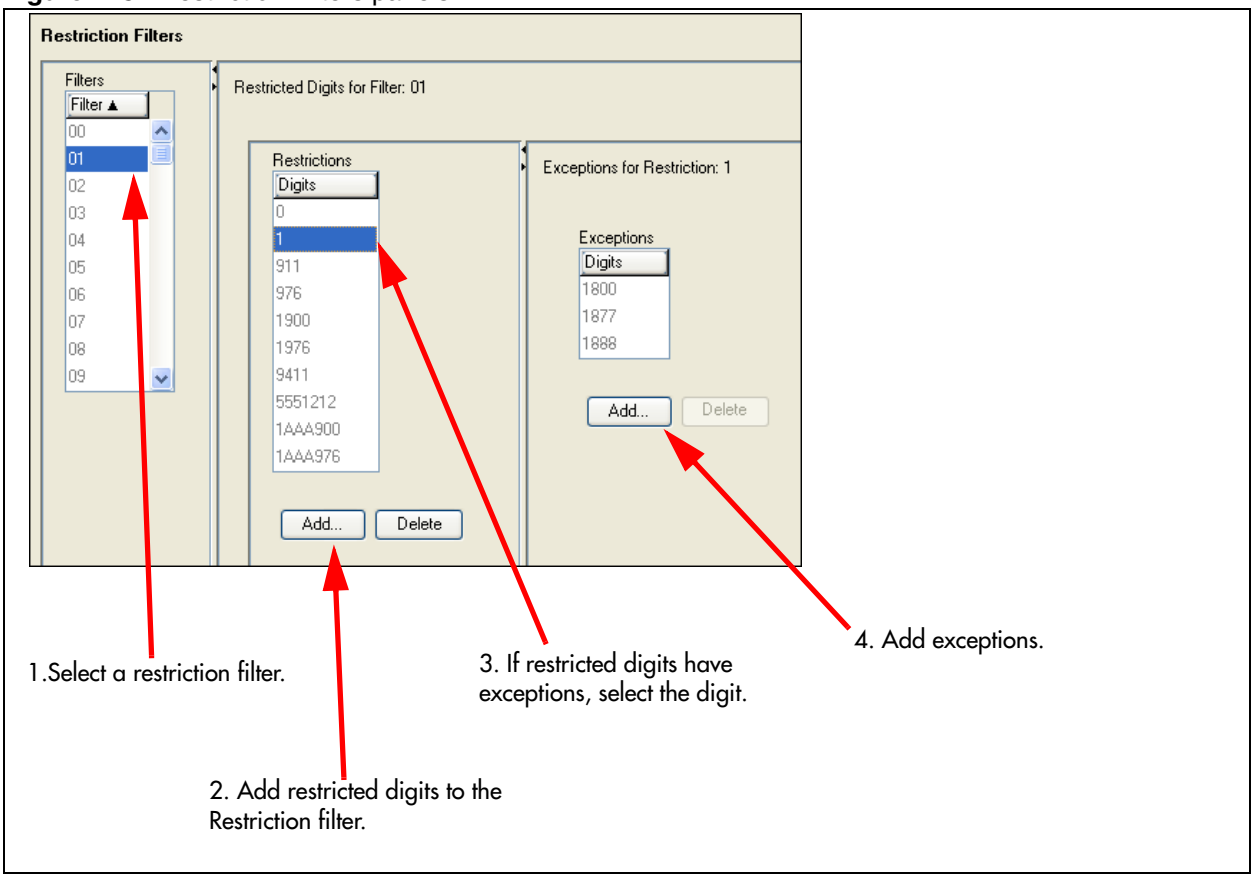


Table 89 provides a description of the fields on the Restriction filters panel.

Table 89 Restriction filters and exceptions fields (Sheet 1 of 2)

Attribute	Value	Description
Filters table		
Filter	<00-99>	This is the list number for the filter. This is the number that you will use on the configuration panels that require restriction filter entries.
Restrictions table		
Digits	<dialstring digit(s)>	For each filter, enter the restriction digit dial string, based on what the restriction is for. The dial string is the number that is restricted from being dialed on the system. Also refer to "Default filters" on page 436. Note: The wildcard *A* (Any) can be used as part of the dialstring.
Actions:		
Add	Refer to "Adding a restriction filter and exceptions" on page 435.	

Table 89 Restriction filters and exceptions fields (Sheet 2 of 2)

Attribute	Value	Description
Delete	1. On the Filters table, select the filter where you want to delete information. 2. On the Restrictions table, select one or more restrictions to delete. 3. Click **Delete**. 4. Click **OK**.	
Exceptions table		
Digits	<dialstring digit(s)>	For each restriction digit, enter any numbers that should dial out, despite the restriction. **Note:** The wildcard *A* (Any) can be used as part of the dialstring.
Actions:		
Add	Refer to "Adding a restriction filter and exceptions" on page 435	
Delete	1. On the Filters table, select the filter where you want to delete information. 2. On the Restrictions table, select the restriction filter that has the exception that you want to delete. 3. On the Exceptions table, click one or more of the exceptions. 4. Under the Exceptions table, click **Delete**. 5. Click **OK**.	

The default values for restriction filters are based on country profile. Refer to "Default filters" on page 436 and "Default filters for other common profiles" on page 437.

Adding a restriction filter and exceptions

To add a restriction filter

1. On the Filters table, select the number for the Restriction Filter where you want to add filters.
2. Under the Restrictions table, click **Add**.
3. Enter the digits that you want to restrict if they precede a dial string going out of the system.
4. Click **OK**.
5. Repeat steps 3 and 4 for all filters you want to add.
6. If you need to apply overrides to a filter, on the Restricted table, click the restricted digit to which you want to add overrides.
7. Under the Exceptions table, click **Add**.
8. Enter the number that you want to allow when this restriction is in effect.
9. Repeat steps 7 and 8 for all overrides you want to add to this filter.
10. Repeat steps 6 to 9 for all the filters to which you want to add overrides.

11 Click **OK**.

12 Next steps: Assign filters to lines, DN records and class of service (CoS) passwords for remote access.

Default filters

The following provides a list of the default restriction filters for North America and other common profiles:

- "Default filters for the North America profile" on page 436
- "Default filters for other common profiles" on page 437

Default filters for the North America profile

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with 10 restrictions and some associated overrides. In Filter 01, Restriction 02 and Override 001 allow long distance toll free calls.

The dialing string 911, which is the number for emergency assistance in North America, is included as both a restriction and an override in Filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Table 90 Default restriction filters

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
01	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Note: Default filters are loaded when the system is initialized. A cold start restores the default filters.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are the default filters in these programming headings:

Filter	Heading	Sub-heading
02	System DNs	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Default filters for other common profiles

Three profiles have global overrides which do not appear in Element Manager restriction programming and cannot be changed.

Australia: 000, 13144A

UK: 999, 112

Chapter 55
Call security: Remote access packages

This panel describes the telephony configuration that is used to control access to system lines by calls coming in from outside the system.The remote access package also allows remote paging capabilities.

Note: Callers dialing into the system over private network lines are also considered remote callers.

The following paths indicate where to access remote access packages in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Call Security > Remote Access Packages**
- Telset interface: ****CONFIG > System prgrming > Remote Access**

This is a two-table panel, where you select a Remote Access Package number on the first panel and then add or delete the line pools from the second table.

Panels/Subpanels	Tasks
"Configuring remote access packages" on page 439	"Restrictions (Line and Remote)" on page 137 (lines)
Also refer to:	"Call Security: Configuring Direct Inward System Access (DISA)" on page 427 "Configuring CoS passwords for remote access" on page 443
Click the navigation tree heading to access general information about Hospitality services.	

Configuring remote access packages

Use these panels to add allowed line pools to up to 99 remote access packages.

Remote access packages are assigned to lines and class of service (CoS) passwords. Lines used for private networking need remote access packages because calls coming from other nodes on the network are considered remote call-ins by your system.

Figure 126 Remote Access Packages tables

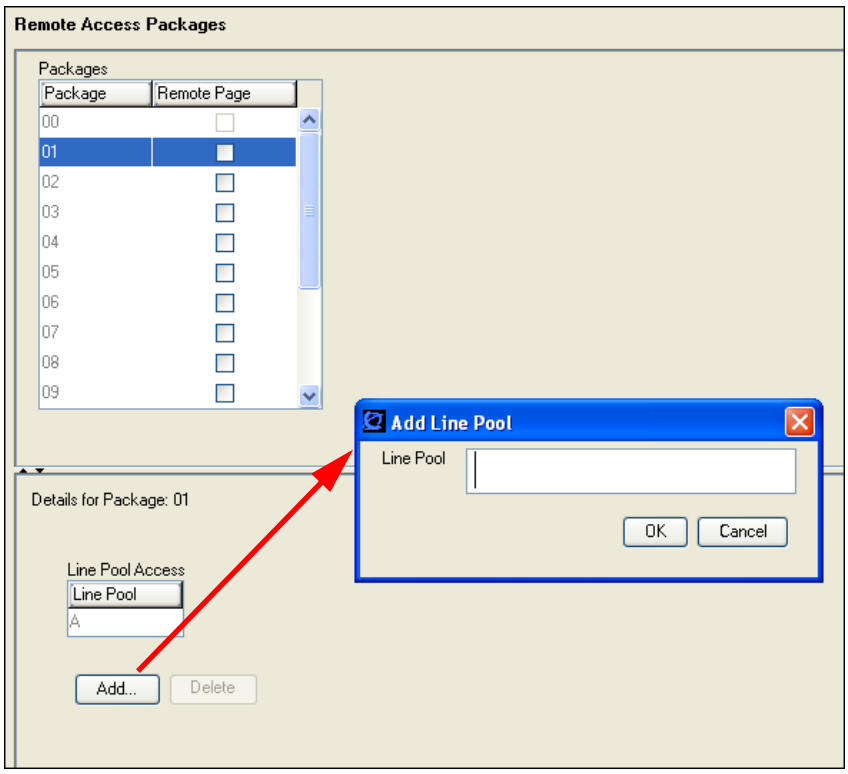


Table 91 describes each field on this panel.

Table 91 Remote Access Packages (Sheet 1 of 2)

Attribute	Values	Description
Packages table		
Package	<00-99>	This designates the package number. This is what is entered in the fields for lines programming for remote access.
Remote Page	<check box>	Select check box if you wish to allow remote callers access to paging. **Note: Remote paging is not supported on IP trunks.**
Line Pool Access table		
Line pool	<A to O>/BlocA to F (PRI and VoIP)	Choose the line pool for which you want this package to be available.
Actions		
Add (line pool)	Package 00 is the default package and cannot be deleted. It provides no access to any line pools. 1. On the Packages table, select the remote package number that you want to configure. 2. Under the Line Pool Access table, click **Add**. 3. In the Add dialog, enter a line pool. 4. Click **OK** to save the pool. 5. Next steps: Add remote access packages to lines and CoS passwords.	

Table 91 Remote Access Packages (Sheet 2 of 2)

Delete (line pool)	1. On the Packages table, select the remote package number where you want to delete line pools. 2. On the Line Pool Access table select one or more line pools to delete. 3. Click **Delete**. 4. Click **OK**.

The following is an example of how a remote access package works.

- Inbound PRI calls are on line pool BlocA
- Outbound calls are on analog lines using Pool A

If users coming in on the PRI are to be able to access outbound trunks on Pool A then the lines in BlocA must be in a remote package that allows access to Pool A

Chapter 56
Configuring CoS passwords for remote access

The Class of Service panel allows you to configure passwords for system users who will be dialing into the system over a PSTN/private network to use system features, or for users who must bypass local restrictions on telephones.

The following paths indicate where to access the Class of Service settings in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Call Security > Class of Service**
- Telset interface: ****CONFIG > Passwords**

Click one of the following links to connect with the type of information you want to view:

Panel tabs	Tasks/Features
"Class of Service table" on page 443	"External access tones" on page 447
Also refer to:	"Call security: Restriction filters" on page 433 "Call Security: Configuring Direct Inward System Access (DISA)" on page 427 "Call security: Remote access packages" on page 439

Click the navigation tree heading to access general information about user management.

CoS passwords permit controlled access to the system resources by both internal and remote users.

- When an internal user enters a CoS password at a telephone, the restriction filters associated with the CoS password apply instead of the normal restriction filters.
- Similarly, when a remote user enters a CoS password on an incoming auto-answer line, the restriction filters and remote package associated with their CoS password apply instead of the normal restriction filters and remote package.

Class of Service table

Refer to the following CoS information:

- "Notes about CoS passwords" on page 445
- "External access tones" on page 447

Security Note: Change passwords frequently to discourage unauthorized access.

Figure 127 Class of Service table panel

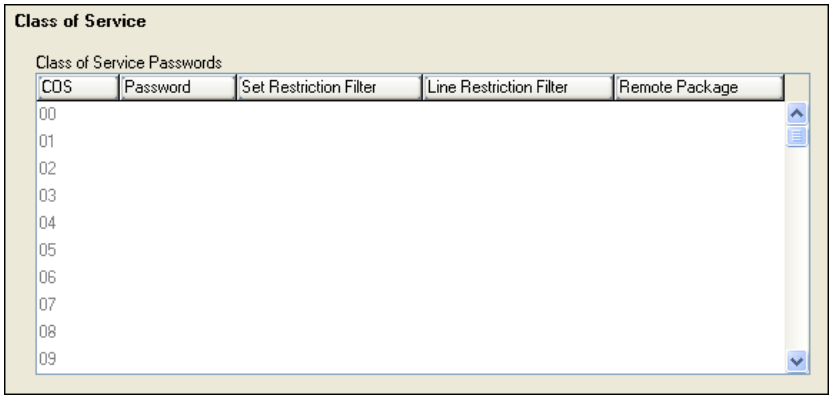


Table 92 describes the fields on this panel.

Table 92 CoS password values

Attribute	Values	Description
CoS	<CoS 00- CoS 99> Read-only	These numbers identify the password position to the system.
Password	<six digits>	Enter a combination of numbers that the user needs to dial to get into the system. Refer to "Notes about CoS passwords" on page 445.
Set Restriction Filter	None Filter <plus a two-digit user filter>	Assign a restriction filter to a Class of Service password. The user filter associated with the Class of Service password replaces any normally-applicable set restriction, line/set restriction, and remote restriction. The default setting (**None**), means that any normally-applicable filters (set restriction, line/set restriction, or remote restriction) still apply.
Line Restriction Filter	None Filter <plus a two-digit line filter>	Assign a specific line restriction to a Class of Service password. The line filter associated with the Class of Service password replaces any normally applicable line restriction. The default setting (**None**), means that any normally applicable line filter still applies.
Remote Package	None Package <plus a two-digit remote package>	Refer to "Call security: Remote access packages" on page 439 for more information.

Adding or modifying a CoS password values

Programming references:

- "Notes about CoS passwords" on page 445

- "External access tones" on page 447

Note: You can add a maximum of 99 CoS Passwords.

To add or modify a CoS password

1 On the Class of Service table, click the CoS line to which you want to add or modify a password.

2 Select the field you want to change and enter the appropriate information:

- Name: Enter a descriptive name for the password or user
- Password: Enter a set of six digits that are unique from any other CoS password
- Set Restriction Filter: If you want the user to be able to override set and line/set restrictions for the number being called, enter the allowed filters.
- Line Restriction Filter: If you want the user to be able to override the line restrictions that the call uses to access the system, enter the allowed filters here.
- Remote Package: Enter the remote package that you want the system to use to determine the level of access the user will have to system features.

Notes about CoS passwords

The CoS password can define the set of line pools that may be accessed and whether or not the user has access to the paging feature. The password all defines which restrictions are applied.

The class of service (CoS) that applies to an incoming remote access call is determined by:

- The filters that you apply to the incoming trunk.
- The CoS password that the caller used to gain access to BCM.
- In cases where DISA is not automatically applied to incoming calls, the remote caller can change the class of service by dialing the DISA DN and entering a CoS password.

Remote users can access system lines, line pools, the Page feature, and remote administration. The exact facilities available to you through remote access vary depending on how your installer set up your system.

Note: Remote paging is not available on IP trunks.

Security Note:
CoS password security and capacity

- Determine the CoS passwords for a system randomly and change them on a regular basis.
- Users should memorize their CoS passwords and keep them private. Typically, each user has a separate password. However, several users can share a password or one user can have several passwords.
- Delete individual CoS passwords or change group passwords when employees leave the company.
- A system can have a maximum of 100 six-digit CoS passwords (00 to 99). CoS passwords must be unique.

To maintain the security of your system, the following practices are recommended:

- Warn a person to whom you give the remote access number to keep the number confidential.
- Change CoS passwords often.
- Warn a person to whom you give a CoS password, to memorize the password and not to write it down.
- Delete the CoS password of a person who leaves your company.

Security note: Remote users can make long distance calls.
Remember that a remote user can make long distance calls that are charged to your company. They can also access line pools and make page announcements in your office.

CoS examples

Example: Using the CoS feature to access a restricted line.

A sales representative out of the office needs to make long distance calls to the European office. Your system has a leased line to Europe with reduced transatlantic charges. You provide the sales representative with a Class of Service password that gives access to the transatlantic line. The sales representative can telephone into the system (DISA DN) from a hotel, enter the Class of Service password, and then use a destination code to access the leased transatlantic line to make calls.

To access the system over a public network

1 Dial the system remote access number.

2 When you hear a stuttered dial tone, enter your CoS password.

3 Wait for the system dial tone.

To bypass the restriction filters on a telephone

1 Press **FEATURE 68**.

2 Enter the six-digit CoS password that allows the required type of call.

3 Enter the number to be dialed.

Example: Remote access over the public network bypassing the restrictions on a telephone

To use the system at a distance, you must use a telephone with tone dialing to call the system. Remote access is possible only on lines that your installer programs to auto-answer calls.

To use paging on a remote system, press * followed by the feature code. When you are calling from within BCM, press * instead of **FEATURE**.

In some conditions, you can experience lower volume levels when using the system from a distance.

External access tones

You can hear some of the following tones when accessing BCM from a remote location. Table 93 shows the different types of tone and what they mean.

Table 93 External access tones (Sheet 1 of 2)

Tone	What it means
System dial tone	You can use the system without entering a CoS password.
Stuttered dial tone	Enter your CoS password.
Busy tone	You have dialed a busy line pool access code. You hear system dial tone again after 5 seconds.

Table 93 External access tones (Sheet 2 of 2)

Fast busy tone	You have done one of the following: • Entered an incorrect CoS password. Your call disconnects after five seconds. • Taken too long while entering a CoS password. Your call disconnects after five seconds. • Tried to use a line pool or feature not permitted by your Class of Service. You hear system dial tone again after five seconds. • Dialed a number in the system which does not exist. Your call disconnects after five seconds.
	IP trunk lines do not produce tones when accessed from a remote location.

Chapter 57
LAN overview

On the BCM main unit, the LAN configuration determines how the Core Module of the BCM communicates with other devices on the LAN. For the BCM with Router, the LAN configuration also includes Router LAN configuration, which determines how the router communicates with devices on the LAN.

The following explains the concepts of the LAN on the BCM. It contains the following topics:

- "What is a LAN?" on page 449
- "LAN settings" on page 449
- "DHCP configuration" on page 449

For information on Configuring LAN settings, see "IP Subsystem" on page 455.

What is a LAN?

The LAN (Local Area Network) is a group of IP devices that can all communicate directly with each other over an IP network. Generally, all of these devices are in a small geographic range, such as a single office or building. The BCM allows you to connect several IP devices together on a LAN and then connect to the Internet or other LANs over a router.

LAN settings

LAN settings include determining IP and DNS settings and subnet settings.The LAN controls how the BCM behaves as a device on the IP network.

To modify the LAN settings, refer to "IP Subsystem" on page 455.

DHCP configuration

By default, the BCM is set as a DHCP client. When the BCM is started, it sends a request for an address to a DHCP server. If no server responds, it determines that there is no DHCP server on the LAN, and it sets a static IP address of the last IP address received from the DHCP server. (The default IP address is 192.168.1.2). Also refer to "DHCP configuration with router" on page 491.

Chapter 58
Configuring the BCM with a DHCP address

To configure the BCM with a DHCP address

1. Set up your DHCP server if it is not already configured on your network. If you are using a BCM50a or BCM50e, consult the router documentation for information on configuring the DHCP network.
2. On your DHCP server, set a reserved address for the BCM. This requires the BCM MAC address, which you can find on the IP subsystem panel or on the stock tag for the box in which the BCM ships. If you do not set a reserved IP address for the BCM, you must change Element Manager clients every time the IP address is reset.
3. Connect the BCM to the network. By default, the BCM detects the presence of a DHCP server and sets itself up as a client of this DHCP server.
   If you plug in the BCM when the DHCP is not available, it will default to a static IP address. You can recover by unplugging the BCM and reconnecting once the DHCP server is available.

Chapter 59
Data networking overview

The BCM is a converged voice product, and can be connected to virtually any data network, to provide Voice over Internet Protocol (VoIP) support in either a Local Area Network (LAN) or Wide Area Network (WAN) environment. The BCM is also available with an integrated Broadband Ethernet or ADSL Router, which is intended to provide basic data networking and services, as well as Virtual Private Network (VPN) connectivity for small sites. Refer to "VPN overview" on page 525 for more information. With the router, the BCM can handle all data networking needs, including both VoIP and basic IP networking. The BCM is also available without a router, to provide VoIP capabilities to networks that already have an existing IP network.

What is data networking?

On the BCM, data networking refers to both standard IP data networks, as well as VoIP. These two types of networks are closely intertwined, and connect a wide range of IP devices - including IP telephones and computers - with the BCM and with external networks. The BCM with router can also handle all routing requirements.

For more information about setting up networks see "System telephony networking overview" on page 33.

About the BCM VoIP capability

The BCM provides VoIP functionality both within a LAN (Local Area Network), and across a WAN. It can contain IP telephones, which act similar to a traditional phone, but send their signals across data networks in the form of IP packets. The BCM can also contain IP trunks which connect offices together across an IP network.

For more information about VoIP see "VoIP overview" on page 363.

Network routing

The BCM is available with and without an internal router. With the router, it can handle all external connections necessary for a data-network, as well as control security on these connections. The standalone version of the BCM does not handle routing, but is suitable for IP networks where a router is already in place. For information on the BCM router see "Router overview" on page 469.

Configuring the BCM with data networks

To configure the BCM to work with a data network, complete the following steps:

- Complete the pre-installation checklist. This will make sure that you've made all necessary preparations for connecting the BCM. For information on completing the pre-installation checklist, "Data network prerequisites checklist" on page 465.
- Configure your router. If you already have a router on your system, you must make some modifications to its configuration for use with the BCM. If you have the BCM50a or BCM50e, you must use the configuration guides for each of those products to set up your router. For information about configuring the Router, refer to the *BCM 4.0a Integrated Router Configuration Guide* (NN40020-500) or the *BCM 4.0e Integrated Router Configuration Guide* (NN40020-501).
- Configure IP settings on the BCM. For information about configuring IP settings on the BCM, refer to "LAN overview" on page 449.
- Configure DHCP on the BCM. For information about configuring DHCP on the BCM, refer to "DHCP overview" on page 475.

Chapter 60
IP Subsystem

The IP Settings define the basic and advanced IP address and DNS configuration for the BCM main unit.

The panel tabs links provide a general description of each panel and definitions of each panel field.

Click one of the following links:

Panel tabs

"Main panel tabs: General settings" on page 455

"Main panel tabs: Internal subnets" on page 458

"Main panel tabs: Dial-out Static Routes" on page 461

Main panel tabs: General settings

The General Settings panel displays the basic IP settings for the BCM main unit. It contains:

- "IP settings options" on page 455
- "DNS Settings options" on page 456
- "MTU option" on page 456

IP settings options

The IP settings options include settings for modifying the IP address information for the BCM.

Modifying IP address information

Warning: Modifying the IP address information for the BCM may cause the BCM to temporarily lose connectivity to the network.

The IP address fields are read-only. However, you can modify their values using the Modify button.

Warning: If any of the IP settings are changed in the modify window for IP settings, the Element Manager will disconnect.

To modify an IP address

1. Click **Configuration > System > IP Subsystem > General Settings** tab.
2. Click **Modify**.
   The **Modify IP Settings** dialog box appears.
3. Enter the appropriate values. See Table 94 for a description of these fields.
4. Click **OK**.
5. You may need to restart your Element Manager to reconnect with the BCM.

DNS Settings options

Enter the DNS Settings options for the BCM to obtain domain name information from a DNS server.

MTU option

BCM allows you to change the MTU based upon your network architecture.

Figure 128 General Settings panel

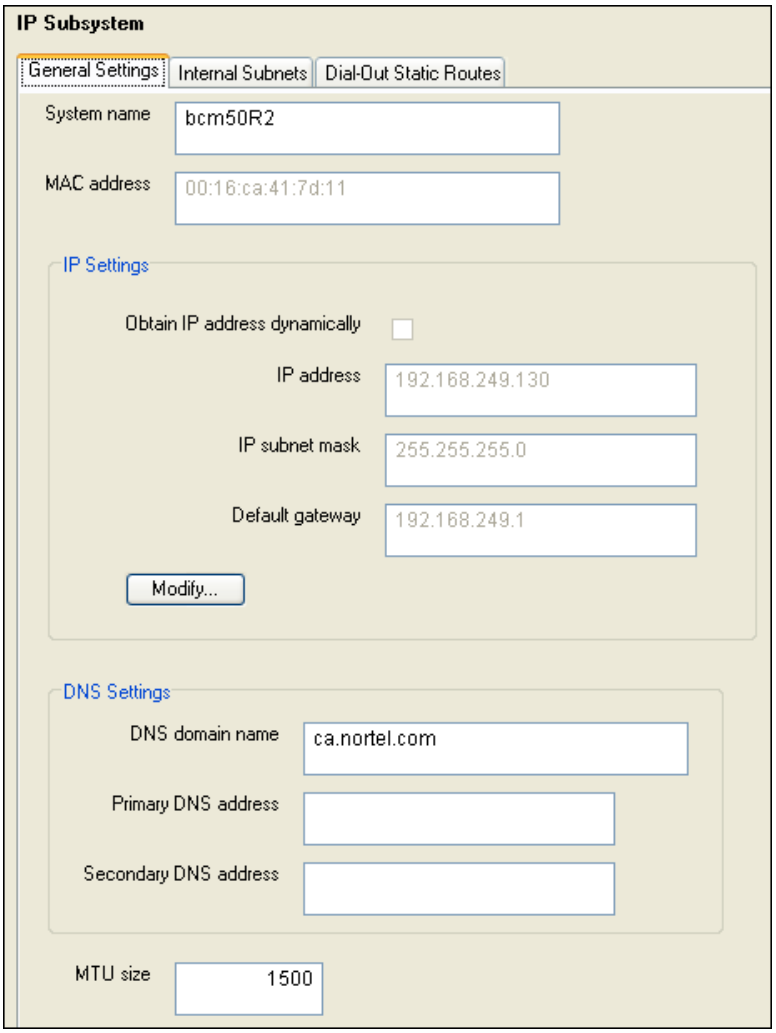


Table 94 General Settings (Sheet 1 of 2)

Attribute	Value	Description
System name	<alphanumeric characters>	Enter a name to identify the BCM.
MAC address	<read-only>	This is the physical address of the BCM core (not the integrated router).
IP Settings		
Obtain IP address dynamically	<check box>	If selected, the BCM obtains IP address information from a DHCP sever. If selected, the IP address and subnet mask are read-only. If not selected, enter the IP address and subnet mask of the BCM.
IP address	<read-only>	The IP address of the BCM main unit.
IP subnet mask	<read-only>	The subnet mask used by the BCM.

Table 94 General Settings (Sheet 2 of 2)

Attribute	Value	Description
Default gateway	<read-only>	The gateway used by the BCM. **Note:** The gateway must be in the same domain, and reachable, from this IP address.
Modify	button	Click **Modify** to change IP settings.
DNS Settings		
DNS domain name	<alphanumeric>	A name for the local domain. You must enter information in this field only if the **Obtain IP address dynamically** check box is not selected.
Primary DNS address	<IP address>	The IP address of the server that will provide DNS information to the system. This information is generally provided by the ISP. This field needs to be completed only if the **Obtain IP address dynamically** check box is not selected. Provided by your ISP or IS department. In small office settings a DNS may not be necessary.
Secondary DNS address	<IP address>	Used if the primary DNS is unavailable. The IP Address of the server that will provide DNS information to the system. This information is generally provided by the ISP. This field needs to be completed only if the **Obtain IP address dynamically** check box is not selected. It can be provided by your ISP or IS department. In small office settings a DNS may not be necessary.
MTU size	<numeric string>	Maximum Transmission Unit. This is the largest packet, measured in bytes, that the BCM can send. **Note**: 1500 is the default setting and should not be changed unless instructed by a network administrator.

Main panel tabs: Internal subnets

The Internal subnets tab contains two subpanels:

- "Internal Subnet settings" on page 458
- "Internal Subnet Details" on page 459

Internal Subnet settings

The Internal Subnets tab contains a table describing the two internal subnets. The OAM LAN provides an interface where administrators can connect directly to the BCM by plugging their laptop into the OAM port.

The Internal LAN is an interface that is used internally by the BCM for digital signal processing.

Warning: Only modify a subnet if the address the subnets are currently set to are in-use elsewhere on the network.

Modifying a Subnet

Warning: You should modify a subnet only if the address the subnet is currently set to are in use elsewhere on the network.

To modify a subnet

1. Click **Configuration > System > IP Subsystem > Internal Subnets** tab.
2. Select the Subnet to modify.
3. Click **Modify**.
   The **Modify Internal Subnet Settings** dialog box appears.
4. Change the settings.
5. Click **OK**.

Internal Subnet Details

The Internal Subnet Details panel contains a table showing the OAM LAN Subnet Details. The details panel displays the DHCP lease of any PC that connects to the OAM port. This table is read-only.

Figure 129 Internal Subnets tab

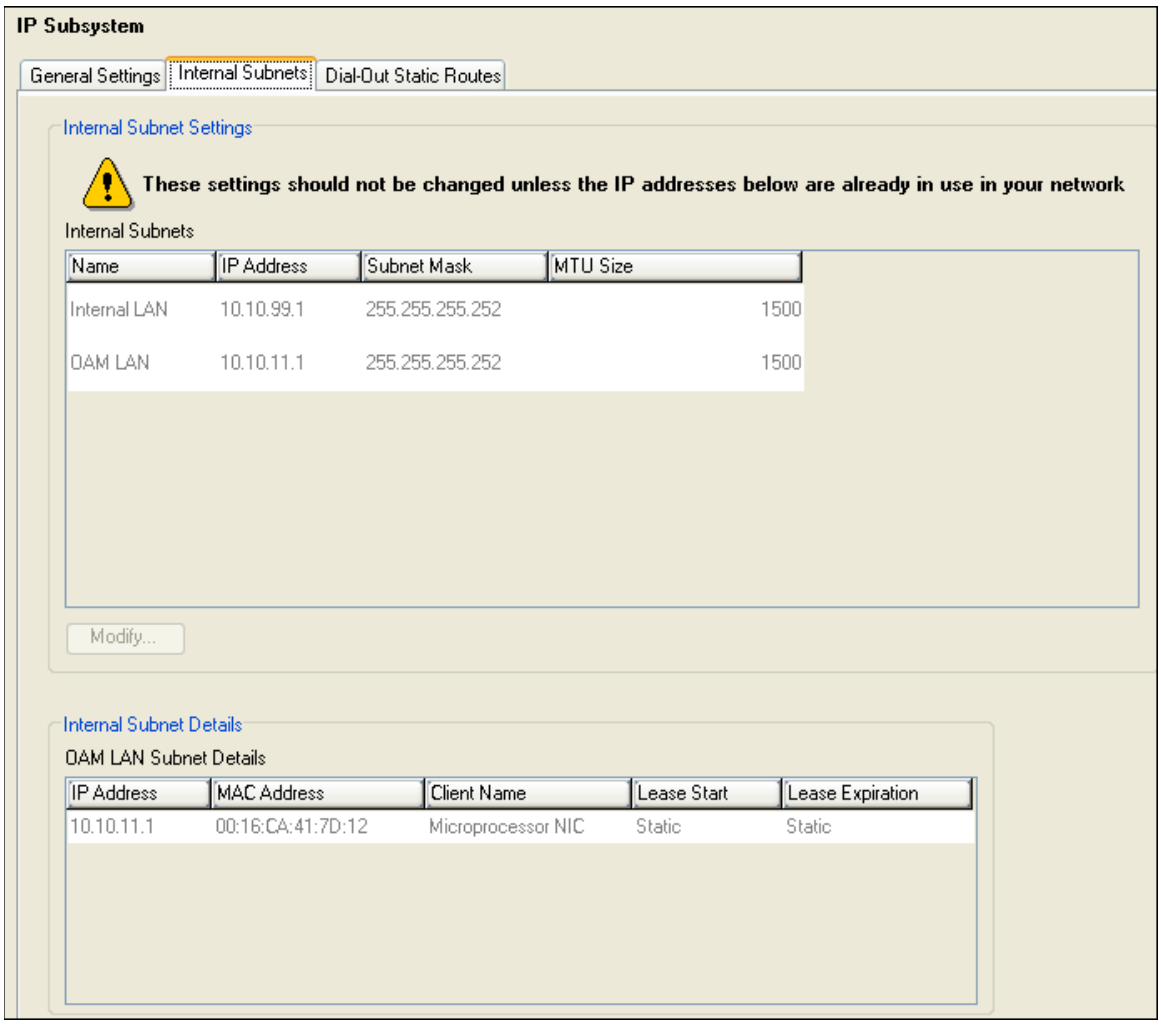


Table 95 Internal Subnets panel (Sheet 1 of 2)

Attribute	Value	Description
Name	<alphanumeric>	The subnet name.
IP Address	<IP address>	The IP address for the subnet.
Subnet Mask	<IP address>	The mask for the subnet.
MTU Size	<numeric string>	Maximum Transmission Size. This is the largest packet, measured in bytes, that the BCM can send.
Internal Subnet Details		
OAM LAN Subnet Details		
IP Address	<IP address>	The IP address for the subnet.
MAC Address	<read-only>	This is the physical address of the BCM (not the integrated router).

Table 95 Internal Subnets panel (Sheet 2 of 2)

Attribute	Value	Description
Client Name	<read-only>	Displayed if client has name in Reserved Addresses table, otherwise blank.
Lease Start	<read-only>	When IP lease began.
Lease Expiration	<read-only>	When IP lease expires.

Main panel tabs: Dial-out Static Routes

Automatic Dial-out Interfaces require static routes. Figure 130 illustrates the Dial-Out Static Routes panel. Refer to Table 96 for a description of the fields.

Figure 130 Main panel tabs: Dial-out Static Routes

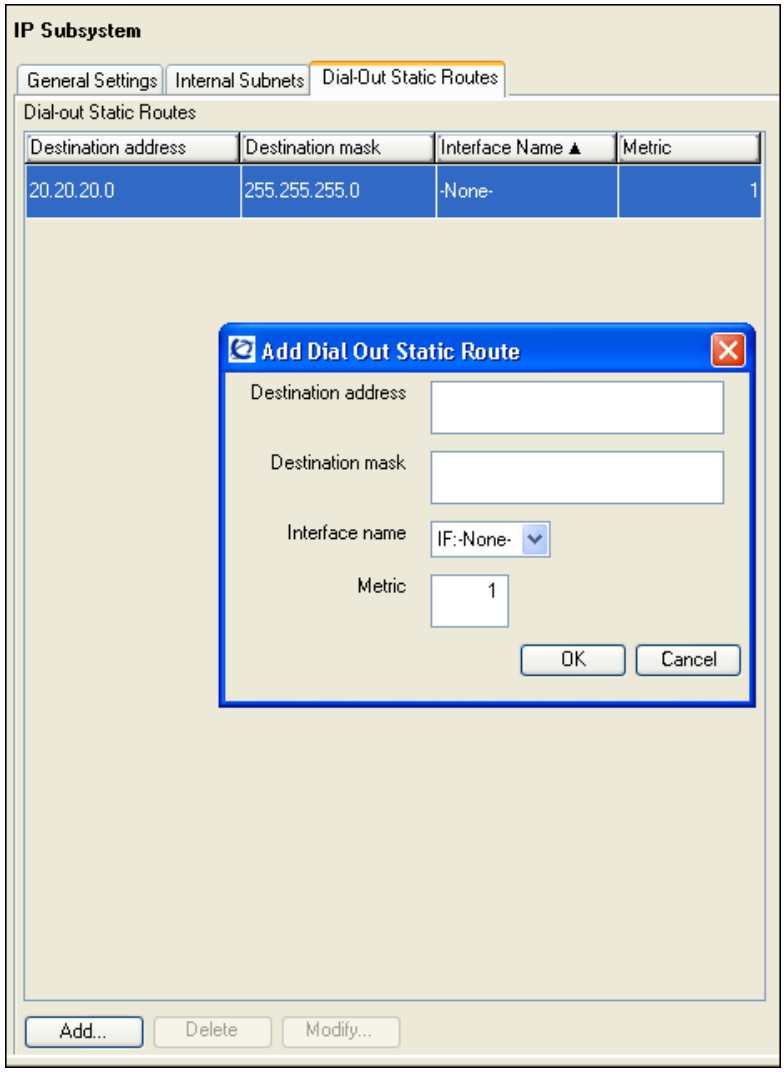


Table 96 Main panel tabs: Dial-out Static Routes

Attribute	Value	Description
Destination Address	<IP Address>	IP address in Ipv4 format. Specify the IP address of the destination network or host. Default: None.
Destination Mask	<IP Address>	Specify the subnet mask of the destination. Default: 255.255.255.0.
Interface Name	<drop-down list>	Choose the dial-out interface to be used by the IP traffic. **Note**: This is a drop-down list with only interfaces that have “Automatic dialout” selected.
Metric Value	<1-32767>	Specify the metric value associated with the interface. 1 means lowest cost and 32767 is the highest cost. Default: 1

Configuring static routes

To add a new IP Static Route

1. Click **Configuration > System > IP Subsystem > Dial-out Static Routes** tab.
2. Click Add.
   The **Add Dial out Static Route** dialog box appears.
3. Enter the Destination, Destination mask, Interface name and Metric fields.
4. Click **OK**.
   The new IP static route appears in the list.

To modify an existing IP Static Route

1. Click **Configuration > System > IP Subsystem > Dial-out Static Routes** tab.
2. Click **Modify**.
   The **Modify Dial out Static Route** dialog box appears.
3. Enter the correct value.
4. Click **OK** to apply the change.

To delete an existing IP Static Route

1. Click **Configuration > System > IP Subsystem > Dial-out Static Routes** tab.
2. Select the Static IP Route you want to delete.
3. Click **Delete**.
   A confirmation dialog box appears.
4. Click **Yes**.

Chapter 61
Data network prerequisites checklist

Before you set up voice over IP (VoIP) trunks or IP telephones on a BCM, complete the following checklists to ensure the system is correctly set up for IP telephony. Some items in the checklist do not apply to all installations.

- "Network diagram" on page 465
- "Network devices" on page 466
- "Network assessment" on page 466
- "Keycodes" on page 467
- "System configuration for IP telephony functions" on page 467
- "VoIP trunks" on page 468
- "IP telephone records" on page 468

Network diagram

To aid in installation, a network diagram provides a basic understanding of how the network is configured. Before you configure IP functionality, create a network diagram that captures all of the information described in Table 97. If you are configuring IP telephones but not VoIP trunks, you do not need to answer the last two questions.

Table 97 Network diagram prerequisites

Prerequisites	Yes
1.a Are you using the BCM50a or BCM50e, and has a network diagram been developed? (If you are not using the BCM50a or BCM50e, it is assumed that the BCM is being installed on an existing network).	
1.b Does the network diagram contain any routers, switches or bridges with corresponding IP addresses and bandwidth values for WAN or LAN links?	
1.c Does the network diagram contain IP Addresses, netmasks, and network locations for all BCM systems and other BCM products?	
1.d Answer this if your system will use IP trunks; otherwise, leave it blank: Does the network diagram contain IP addresses and netmasks of any other VoIP gateways to which you must connect?	
1.e Answer this only if your system will use a gatekeeper; otherwise, leave it blank: Does the network diagram contain the IP address for any Gatekeeper that may be used?	

Network devices

Table 98 contains questions about devices on the network such as firewalls, NAT devices, and DHCP servers.

- If the network uses public IP addresses, complete 2.d.
- If the network uses private IP addresses, complete 2.e. to 2.f.

Table 98 Network device checklist

Prerequisites	Yes	No
2.a Is the network using DHCP?		
2.b If so, are you using the DHCP server on the BCM Router?		
2.c Is the network using private IP addresses?		
2.d Are there enough public IP addresses to accommodate all IP telephones and the BCM?		
2.e Does the system have a firewall/NAT device, or will the BCM be used as a firewall/NAT device?		
2.f If the BCM50a/BCM50e is to be used as a firewall/NAT device, do the firewall rules fit within the 10 input rules and the 10 output rules that the BCM provides?		

Network assessment

Answer the questions in Table 99 to ensure that the network is capable of handling IP telephony and that existing network services are not adversely affected.

Table 99 Network assessment

Prerequisites	Yes	No
3.a Has a network assessment been completed?		
3.b Has the number of switch ports available and used in the LAN infrastructure been calculated?		
3.c Does the switch use VLANs? If so, get the VLAN port number and ID.		
3.d Have the used and available IP addresses for each LAN segment been calculated?		
3.e Has DHCP usage and location been recorded?		
3.f Has the speed and configuration of the LAN been calculated?		
3.g Has the estimated latency values between network locations been calculated?		
3.h Have the Bandwidth/CIR utilization values for all WAN links been calculated?		
3.i Has the quality of service availability on the network been calculated?		

Keycodes

All elements of VoIP trunks and IP telephony are locked by the BCM keycode system. Answer the questions in Table 100 to ensure you have the appropriate keycodes. You can purchase keycodes for the amount of access you want for your system. Additional keycodes can be added later, provided there are adequate resources to handle them. For information about determining the number of keycodes required, see the *Keycode Installation Guide* (NN40010-301).

Table 100 Keycodes

Prerequisites	Yes	No
4.a Complete this question only if you are using VoIP trunks: Do you have enough VoIP keycodes? H.323 trunks use VoIP keycodes.		
4.b Complete this question only if you are using IP telephones: Do you have enough IP client keycodes? (Note: IP clients and IP telephones are a 1:1 ratio. As soon as an IP telephone is registered, it occupies an IP client, whether it is active or not.).		
4.c If you are using VoIP trunks, do you need to activate MCDN features? **Note:** If MCDN is already configured on your system for private networking over PRI lines, you do not need a separate MCDN keycode for VoIP trunks.		

System configuration for IP telephony functions

Several sections of the BCM must be properly configured prior to IP telephony activation. Connect the BCM to the network before completing this checklist. Answer the questions in Table 101 to determine if your BCM has been correctly configured.

Table 101 BCM system configuration

Prerequisites	Yes	No
5.a Is the LAN functioning correctly with the BCM? You can test this by pinging other addresses around the network from the BCM.		
5.b Is the WAN functioning correctly with the BCM50a/BCM50e?		
5.c Have you determined the published IP address for the system?		
5.d Have the necessary media gateway, IP client, and IP trunks resources been set?		
5.e Has a dialing plan been created, taking into account special considerations for IP telephony and private and public networking?		
5.f Have thresholds been set for desktop and soft client IP sets for voice quality monitoring with Proactive Voice Quality Management?		

VoIP trunks

Answer the questions in Table 102 if you are configuring VoIP trunks.

Table 102 VoIP trunk provisioning

Prerequisites	Yes	No
6.a Have you confirmed the remote gateway settings and access codes required?		
6.b Have you determined the preferred codecs required for each type of trunk and destination?		
6.c Have you set up line parameters, determined line pools for H.323 trunks, and set up destination codes? Have you determined which system telephones will have access to these routes?		
6.d If you have not already assigned target lines, have you defined how you are going to distribute them on your system?		
6.e Have you decided if you are going to employ the fallback feature? If yes, ensure that your routing and scheduling are set up. Ensure that QoS is activated. If either of these conditions is not met, your H.323 trunks will not work correctly.		

IP telephone records

Answer the questions in Table 103 if you are installing i-series telephones.

Table 103 IP telephone provisioning

Prerequisites	Yes	No
7.a Are IP connections and IP addresses available for all IP telephones?		
7.b If DHCP is not being used, has all telephone configuration been documented and made available for telephone installers? Hint: Use the Programming Record form.		
7.c If DHCP is not being used, or if you want to enter the port manually, has the VLAN port number been supplied, if one is being used on the switch?		
7.d Have telephone power and connectors been provisioned?		
7.e Do computers that will be using the Nortel Software Phone IP softphone 2050 meet the minimum system requirements, including headset? **Note**: Additional details available on client page for BCM		
7.f Have DN records been programmed for the corresponding IP clients? (Use when manually assigning DNs to the telephones.)		

Chapter 62
Router overview

The following introduces the router, available with the BCM, and explains the two different types of routers available. As well, it introduces the key features you must configure on your router.

For more information on the router, see your router documentation.

The router is a fully functional and powerful device that connects your LAN to an external data network. In addition to configuring and connecting your LAN and WAN, it provides a wide range of data services including Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), firewalls, and Virtual Private Networks (VPN). See "VPN overview" on page 525 for more information.

ADSL and Ethernet configurations

The BCM with router is available in two versions:

- BCM50a: The BCM with an ADSL modem. This version connects to external networks over an ADSL modem within the router.
- BCM50e: The BCM with Ethernet. This version connects to external networks over an Ethernet connection.

Router features

The router offers a wide range of features ranging from DHCP, Firewall, NAT, and VPN. For more information see the *BCM 4.0a Integrated Router Configuration Guide* (NN40020-500) and the *BCM 4.0e Integrated Router Configuration Guide* (NN40020-501).

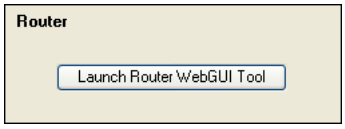
Chapter 63
Router panel

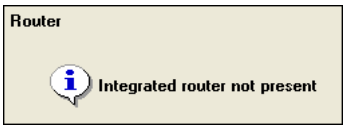
Use the router panel to launch the router on your BCM50a/BCM50e.

For information about configuring the router, consult the router documentation.

Note: The Launch Router button will appear only if you have a BCM50a/BCM50e.

Figure 131 Router panel display





Accessing your router

To access your router

1 Click **Launch Router WebGUI Tool**.
The Contivity Router interface appears in a new window.

Note: The BCM uses the default gateway setting as your router IP address to launch the router WebGUI tool from Element Manager. If the default gateway is not set to the router IP address, you must access the router WebGUI directly from a web browser.

Chapter 64
VLAN overview

A virtual LAN (VLAN) is a logical grouping of ports, controlled by a switch, and end-stations, such as IP telephones, configured so that all ports and end-stations in the VLAN appear to be on the same physical (or extended) LAN segment even though they may be geographically separated. VLAN IDs are determined by how the VLAN switch is configured. If you are not the network administrator, you must ask whoever manages the switch what the VLAN ID range is for your system.

VLANs aim to offer the following benefits:

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of move, add, and change in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.
- For IP telephony, VLANs provide a useful technique to separate and prioritize the telephony traffic for L2 switches.
- VLAN also provides a shield from malicious traffic that may be targeted at the IP phone in order to steal or disrupt service.
- Reuse IP addresses in different VLANs.
- As far as possible, VLANs maintain compatibility with existing bridges and end stations.
- If all bridge ports are configured to transmit and receive untagged frames, bridges will work in plug-and-play ISO/IEC 15802-3 mode. End stations are able to communicate throughout the Bridged LAN.

Choosing DHCP for VLAN

By using the BCM DHCP server, you can configure DHCP to auto-assign a VLAN ID to each IP telephone that registers. With this configuration, you can also choose to manually enter VLAN IDs, if you choose. The BCM DHCP server becomes the default VLAN that everyone can reach. The server provides the network configuration information in the default VLAN, and it also provides the VLAN information for the network.

Specifying the site-specific options for VLAN

The BCM DHCP server resides in the default VLAN and is configured to supply the VLAN information to the IP phones. The DHCP server supplies site-specific options in the DHCP offer message.

The following definition describes the Nortel IP Phone 2004-specific, site-specific option. This option uses the **reserved for site specific use** DHCP options (DHCP option values 128 to 254) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone 2004 to accept these messages as valid. The IP Phone 2004 pulls the relevant information out of this option and uses it to configure the IP phone.

Format of field is: Type, Length, Data.

Type (1 octet):

- Five choices 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251).
- Providing a choice of five types allows the IP Phone 2004 to work in environments where the initial choice may already be in use by a different vendor. Select only one TYPE byte.

Length (1 octet): (variable depends on the message content)

Data (length octets):

- ASCII based
- format: `VLAN-A:XXX,YYY.ZZZ.`

  where `VLAN-A:` uniquely identifies this as the Nortel DHCP VLAN discovery.

  — `-A` signifies this version of this spec. Future enhancements could use `-B`, for example.

  — ASCII `,` (comma) is used to separate fields.

  — ASCII `.` (period) is used to signal end of structure.

  — `XXX`, `YYY` and `ZZZ` are ASCII-encoded decimal numbers with a range of 0-4095. The number is used to identify the VLAN Ids. A maximum of 10 VLAN Ids can be configured. `NONE` means no VLAN (default VLAN).

The DHCP Offer message carrying VLAN information has no VLAN tag when it is sent out from the DHCP server. However, a VLAN tag is added to the packet at the switch port. The packets are untagged at the port of the IP phone.

Chapter 65
DHCP overview

On the BCM, DHCP can be set up in a variety of configurations, based on your needs, your existing network, and the version of the BCM that you have.

The following explains the various ways that you can configure DHCP on the BCM (including router and main configuration).

- "Understanding DHCP" on page 475
- "DHCP network scenarios" on page 476
- "Default configurations" on page 478

Understanding DHCP

Dynamic Host Configuration Protocol (DHCP) is a protocol used to assign IP addresses to devices on an IP network dynamically. With DHCP, each device obtains a new IP address every time it connects to the network. DHCP allows a server to keep track of the IP addresses for all IP devices on the network.

On the BCM, DHCP reduces the complexity of configuring IP devices, particularly IP phones. Not only do IP phones receive an IP address through DHCP, they also receive additional information such as gateway and port information.

DHCP on the BCM

The BCM uses DHCP in a variety of ways. The core of the BCM has a DHCP server. In addition to providing IP addresses to devices on the LAN, this DHCP server also provides a DHCP address to the OAM port and to the DSP LAN.

If you have a BCM with a router, the router also has a DHCP server that provides addresses to devices on the LAN. If the DHCP server on the embedded router is enabled, you will not be able to configure the DHCP settings on the BCM. This prevents situations where the two DHCP servers might conflict with one another.

In addition to these two DHCP components, the BCM is also designed to work with other DHCP devices that may already be on the network.

Router DHCP Server

Both the BCM50a and the BCM50e have a DHCP server.

If you intend to use the BCM50a or BCM50e as a DHCP server, configure the router to be the DHCP server, as described in the *BCM 4.0a Integrated Router Configuration Guide* (NN40020-500) or the *BCM 4.0e Integrated Router Configuration Guide* (NN40020-501). The main module disables its own DHCP server if the route-embedded DHCP server is active.

Main Module DHCP client

The main module can act as a DHCP client. As a DHCP client, the Core Module gets an IP address from another DHCP server on the network. If no other DHCP server is available, the Main Module uses a static IP address, if one is provided.

Main Module DHCP server

The main module has a DHCP server that provides DHCP and vendor-specific information to IP sets. It also provides DHCP information to other devices on the LAN, in the event that no other DHCP Server, such as a router, is available.

DHCP network scenarios

These network scenarios explain the BCM DHCP functionality.

No external DHCP server

With the DHCP Status set to **Enabled (Automatic)**, which is the default, the BCM first attempts to get a dynamic IP address from a DHCP server. When it does not get a response, it uses the IP address 192.168.1.2/255.255.255.0. The system goes through the process of looking for a dynamic IP address each time it reboots. By default, the DHCP server is setup to give out an address range of 192.168.1.200 - 192.168.1.254.

The BCM DHCP server services all devices requesting DHCP information, such as NortelIP phones and PCs. This is equivalent to setting the DHCP Status to **Enabled (All Devices)**.

In this situation, the default VoIP settings are:

- S1 IP address: 192.168.1.2
- S1 Port number: 7000
- S1 Action: 1
- S1 Retry count: 1
- S2 IP address: 192.168.1.2
- S2 Port: 7000
- S2 Action: 1

- S2 Retry count: 1

With external DHCP server

With the DHCP Status set to **Enabled (Automatic)**, which is the default, the BCM first attempts to get a dynamic IP address from a DHCP server. The external DHCP server responds with an IP address, for example 47.166.50.108/255.255.255.192, as well as domain information such as europe.nortel.com.

If the BCM receives an address assignment from a DHCP server, the BCM DHCP Server services only Nortel IP Phones requesting DHCP information. It does not service PCs. This is equivalent to setting the DHCP Status to **Enabled (IP Phones Only)**.

The VoIP settings allow any Nortel IP telephone using DHCP to get the BCM address and connect to the system:

- S1 IP address: 47.166.50.108
- S1 Port: 7000
- S1 Action: 1
- S1 Retry count: 1
- S2 IP address: 47.166.50.108
- S2 Port: 7000
- S2 Action: 1
- S2 Retry count: 1

BCM is unable to reach external DHCP server

In an instance where a BCM is unable to connect the DHCP server it had previously been using, it uses configuration information that exists from the previous lease. After the BCM is unable to get a dynamic IP address from a server, it uses the IP address saved from the previous lease. The VoIP information remains unchanged, since the IP address for the BCM LAN has not changed. The BCM still attempts to renew it's dynamic IP address each time it reboots, so if the external DHCP server becomes available again, it will get a new dynamic IP address.

BCM using a dynamic address is changed to a static address

If a BCM had been using a dynamic IP address, and is manually changed to use a static IP address, the VoIP information for the BCM LAN changes as well.

For example, the BCM LAN IP address, S1 and S2 IP address were all set to 47.166.50.80. When the BCM LAN IP address is changed to a static IP address 47.166.50.114, the S1 and S2 IP addresses also change to 46.166.50.114. If the S1 or S2 IP addresses was set manually and is different from the BCM customer LAN address, these addresses will not be updated.

DHCP server on BCM50a and BCM50e

The BCM50a and BCM50e include a router with a DHCP server. By default, this DHCP server will provide a dynamic IP address to the BCM Customer LAN. The embedded router will recognize the MAC address of the BCM and reserve an IP address (192.168.1.2 is the default address).

When the BCM requests a dynamic IP address, the embedded router sends the reserved IP address, and disables the DHCP server on the BCM.

The embedded router supplies DHCP information as well as the vendor information for IP sets. If the reserved IP address for the BCM matches the S1 or S2 address and is changed, the VoIP information changes as well. If the S1 or S2 IP address have been set manually and are different from the BCM address, these addresses are not updated.

For example, a system has a BCM LAN IP address of 47.166.50.108, an S1 IP address of 47.50.22.34, and an S2 IP address of 47.166.50.108. If the BCM LAN IP address is changed, the S2 IP address changes as well, because it had matched the BCM LAN IP address. The S1 IP address does not change, because it had been set manually.

Whenever the BCM LAN IP address changes, the IP sets eventually detect this and reset themselves if they are using DHCP. If they are manually configured, then each set must be re-configured to point to the new BCM IP address. They will get the new VoIP information from the embedded router, which provides them with the new IP address for the BCM.

Default configurations

The DHCP component is designed with an automatic configuration that should work in most environments.

If the BCM includes a router, the router is by default the DHCP Server.

The core module is by default a DHCP client. It attempts to obtain its IP address over DHCP.

The core module DHCP Server setting is by default set to ‘automatic’. The result of the DHCP client’s request determines the functionality of the DHCP Server.

If it is successful in obtaining an IP address, the BCM turns on its DHCP Server to supply addresses to IP sets only. It will ignore DHCP requests from other IP devices, allowing those requests to be handled by the other DHCP Server on the network.

If it is unsuccessful in obtaining an IP address, the BCM turns off its DHCP client, and turns on its DHCP Server to supply addresses to all devices that request IP addresses.

Additional settings to configure

In addition to these default settings, you must also configure several other settings, including DNS and WINS server settings, and IP set information.

Chapter 66
DHCP Server Settings panel

The DHCP Server Settings contains fields for configuring the BCM core as a DHCP server.

Note: The DHCP settings panel is unavailable for the BCM50a or BCM50e if DHCP is enabled on the embedded router. In that case, the DHCP Server Settings panel is replaced by a single button that opens the GUI for the embedded router.

The DHCP Server Settings panel is a multi-layered, multi-tabbed panel.

The panel tabs links provide a general description of each panel and definitions of each panel field.

Click one of the following links:

Panel tabs

"Main panel tabs: General Settings" on page 481

"Main panel tabs: IP Terminal DHCP Options" on page 483

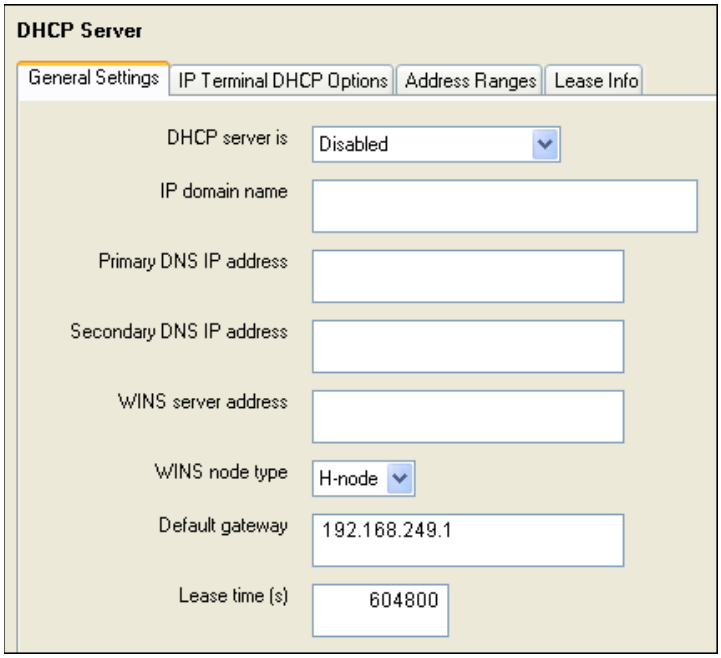
"Main panel tabs: Address Ranges" on page 486

"Main panel tabs: Lease Info" on page 489

Main panel tabs: General Settings

The General Settings tab controls the main DHCP settings including WINS and DNS settings.

Figure 132 General Settings tab



Warning: Whenever you make changes to the default gateway, the DHCP server may become unavailable to clients for a brief period of time. When making changes, consider doing so at a time that will minimize the effect on users.

Table 104 General Settings (Sheet 1 of 2)

Attribute	Value	Description
The DHCP Server is	Disabled Enabled - IP Phones Only Enabled - All Devices Enabled - Automatic	Determines the functionality of the DHCP server. Default: Disabled
IP domain name	<alphanumeric character string>	The domain name of the network.
Primary DNS IP address	<IP Address, format 10.10.10.10>	The IP address of the primary DNS to be used by DHCP clients.
Secondary DNS IP address	<IP Address, format 10.10.10.10>	The IP address of the secondary DNS to be used by DHCP clients.
WINS server address	<IP Address, format 10.10.10.10>	The address of the Windows Internet Server, which resolves IP addresses on a DHCP network.

Table 104 General Settings (Sheet 2 of 2)

Attribute	Value	Description
WINS node type	<drop-down menu>	The type of WINS node: • B-node: The BCM first checks the HMHOSTS cache, then uses broadcast for name registration and resolution. • P-node: The BCM registers with a NetBIOS Name server at startup. • M-node: Mixes B- and P-node. The BCM uses the B-node method, and if that fails, uses the P-node method. • H-node: Uses both B- and P-node methods. B-node is used only as a last resort. Default: H-node
Default gateway	<IP Address, format 10.10.10.10>	The gateway through which DHCP clients connect to an external network. Generally, this is the IP address of the BCM router.
Lease time(s)	<numeric string>	The amount of time before a DHCP lease expires and the device must request a new IP address. Default: 604800 seconds

Main panel tabs: IP Terminal DHCP Options

The IP Terminal DHCP Options settings must be enabled for the IP Phones to function properly. If the system does not use IP Phones or if partial DHCP is enabled, this tab does not need to be configured.

The IP Terminal DHCP Options tab has three subpanels: Primary Terminal Proxy Server, (S1) Secondary Terminal Proxy Server (S2), and VLAN.

Primary Terminal Proxy Server options

The Primary Terminal Proxy Server settings specify information that is sent with the DHCP lease, giving additional information to IP telephones.

Secondary Terminal Proxy Server options

The Secondary Terminal Proxy Server settings control a fallback option in the event that an IP phone is unable to connect with the Primary Terminal Proxy Server. The settings for the Secondary Terminal Proxy Server are the same as those for the Primary Terminal Proxy Server.

VLAN options

If you are using a router that supports VLAN, you can configure the BCM as a VLAN member by entering a VLAN string into this field. This identifier is sent out to all IP terminals along with their DHCP information.

Figure 133 IP Terminal DHCP Options

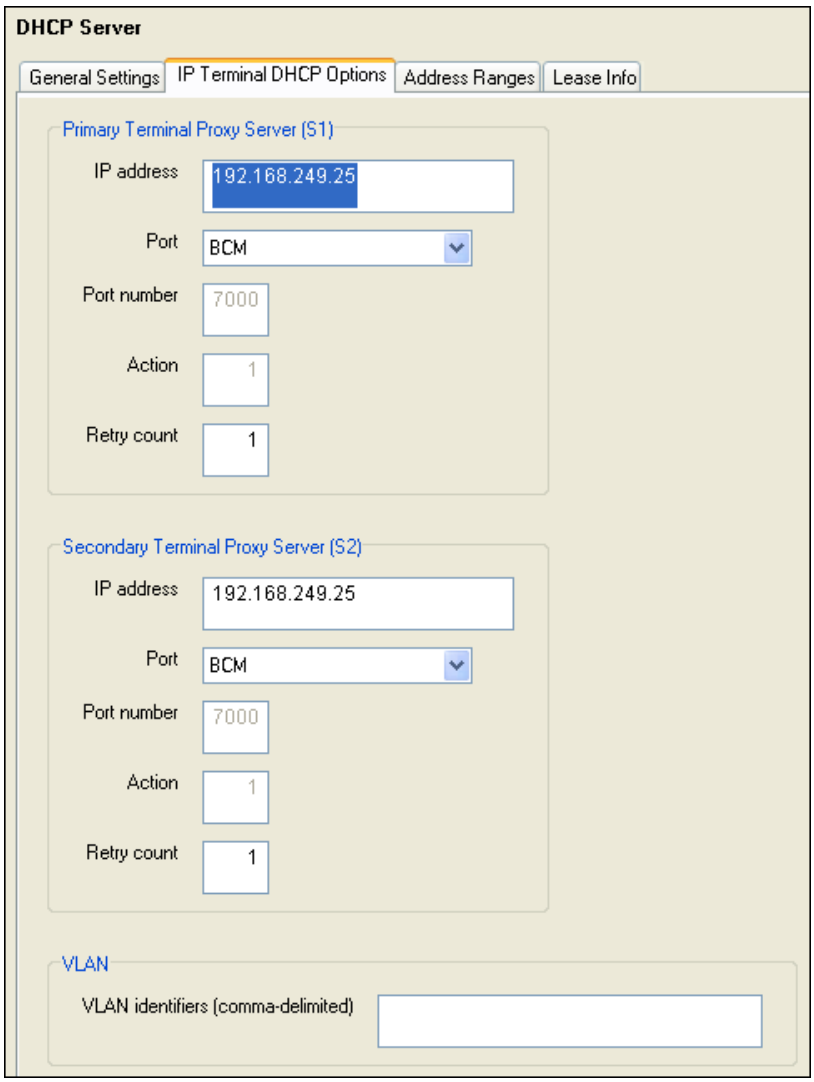


Table 105 IP Terminal DHCP Options (Sheet 1 of 2)

Attribute	Value	Description
Primary Terminal Proxy Server (S1)		
IP Address	<IP address> 10.10.10.10	The IP address of the Proxy Server for IP phones.
Port	<drop-down list>	Select the appropriate port: BCM SRG Meridian 1/Succession 1000 Centrex/SL-100 Other
Port number	<number>	The port number on the terminal through which IP phones connect.

Table 105 IP Terminal DHCP Options (Sheet 2 of 2)

Attribute	Value	Description
Action	<read-only>	The initial action code for the IP telephone.
Retry count	<number>	The delay before an IP phone retries connecting to the proxy server.
Secondary Terminal Proxy Server (S2)		
IP address	<IP address> 10.10.10.10	The IP address of the Proxy Server for IP phones.
Port	<drop-down list>	Select the appropriate port: BCM SRG Meridian 1/Succession 1000 Centrex/SL-100 Other
Port number	<number>	The port number on the terminal through which IP phones connect.
Action	<read-only>	The initial action code for the IP telephone.
Retry count	<number>	The delay before an IP phone retries connecting to the proxy server.
VLAN		
VLAN identifiers (comma-delimited)		Specify the Virtual LAN (VLAN) ID numbers that are given to the IP telephones. If you want DHCP to automatically assign VLAN IDs to the IP telephones, enter the VLAN IDs in the following format: **VLAN-A:id1, id3,...,idn**. where: VLAN-A is an identifier that tells the IP telephone that this message is a VLAN discovery message. id1, id2,...idn are the VLAN ID numbers that DHCP can assign to the IP telephones. You can have up to 10 VLAN ID numbers listed. The VLAN ID numbers must be from 0 to 4095. For example, if you wanted to use VLAN IDs 1100, 1200, 1300 and 1400, you would enter the following string in this box: **VLAN-A:1100, 1200, 1300, 1400**. If you do not want DHCP to automatically assign VLAN IDs to the telephones, enter **VLAN-A:none**, in this text box. **Note1**: The NORTEL IP Terminal VLAN ID string, must be terminated with a period (.). **Note2**: If you do not know the VLAN ID, contact your network administrator. **Note3**: For information about how to set up a VLAN, refer to the user documentation that came with your VLAN compatible switch.

Main panel tabs: Address Ranges

Warning: Whenever you make changes to the address range, the DHCP server may become unavailable to clients for a brief period of time. When making changes, consider doing so at a time that will minimize the effect on users.

The Address Ranges tab specifies IP addresses to be provided to DHCP clients. The Address Ranges tab has two tables: Included Address Ranges and Reserved Addresses.The Included Address Ranges specifies a range of IP addresses to be provided to DHCP clients.

DHCP subnets

By default, the DHCP server on the BCM must configure a range of IP addresses to supply the IP sets. It defaults to use the top 20 percent of a subnet. For example, if an external DHCP server supplies the following IP address to the BCM: 177.218.21.45/255.255.255.0, then the BCM DHCP server configures itself to reserve the following range 177.218.21.200-177.218.21.254.

You can use Element Manager to check and change this default. The Reserved Addresses table lists IP addresses that are reserved for specific clients. These IP addresses can fall within an Included Address Range, or they can be outside any Included Address Ranges.

Figure 134 Address Ranges tab

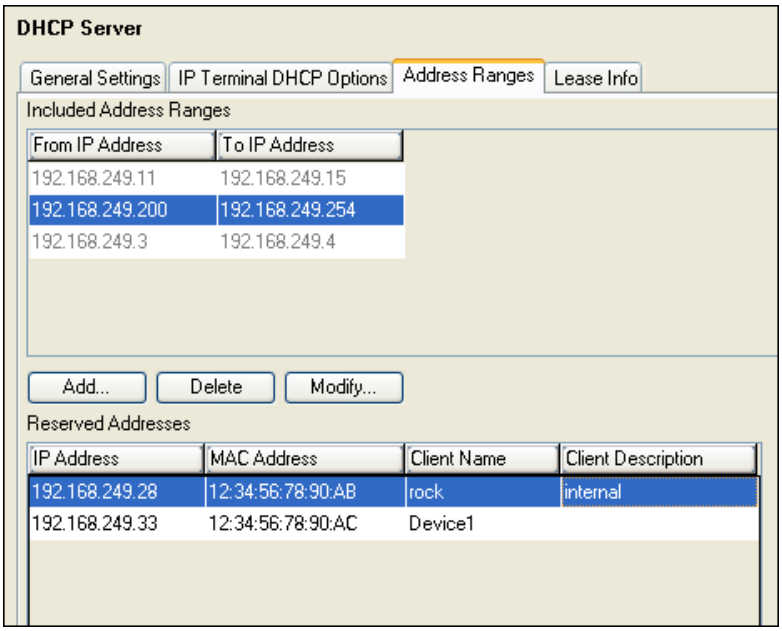


Table 106 Address Ranges

Attribute	Value	Description
Included Address Ranges		
From IP Address	<IP Address, format 10.10.10.10>	An IP address specifying the lowest IP address in a range.
To IP Address	<IP Address, format 10.10.10.10>	An IP address specifying the highest IP address in a range.
Add	<button>	Click to add an included address range.
Delete	<button>	Click to delete a selected address range.
Modify	<button>	Click to modify a selected address range.
Reserved Addresses		
IP Address	<IP address>	Specify the IP Address that is reserved for this DHCP client.
MAC Address	<IP address>	Specify the MAC address for the DHCP client to which this IP address is assigned. The permitted values is 6 bytes in hexadecimal format.
Client Name	<alphanumeric>	Specify the name of the DHCP client.
Client Description	<alphanumeric>	Specify the description that will help to identify the DHCP client to which this IP address is assigned.
Add	<button>	Click to add a reserved address.
Delete	<button>	Click to delete a reserved address.

To add a new Included Address Range

1. Click **Configuration > Data Services >DHCP Server > Address Ranges.**
2. Click **Add** beneath the Included Address Ranges table.
   The **Add Included Address Range** dialog box appears.
3. Enter the appropriate **From IP address** and **To IP address** ranges.
4. Click **OK**.
   The address range is added to the table.

To delete an Included Address Range

1. Highlight the Address Range you want to delete.
2. Click **Delete**.
3. Click **Yes** on the confirmation dialog box.

To add a Reserved Address

1. Click **Configuration > Data Services >DHCP Server > Address Ranges.**
2. Click **Add** beneath the Reserved Address table.
   The **Add Reserved Address** dialog box appears.
3. Enter the appropriate information in the IP address, MAC address, Client name, and Client description fields. The IP Address and MAC Address are required fields. The Client Name and Client Access are optional fields.
4. Click **OK**.
   The reserved address is added to the table.

To delete a Reserved Address

1. Highlight the Reserved Address you want to delete.
2. Click **Delete**.
3. Click **Yes** on the confirmation dialog box

Note: You cannot exclude addresses in an address range. Instead, you can use multiple address ranges:

1. Create one address range for the IP addresses below the excluded addresses.
2. Create a second address range for the IP addresses above the excluded addresses.

For example, to create an address range from 10.10.10.10 to 10.10.10.49, but excluding addresses from 10.10.10.20 to 10.10.10.29, create one address range from 10.10.10.10 to 10.10.10.19 and one address range from 10.10.10.30 to 10.10.10.49.

Main panel tabs: Lease Info

The lease info panel is a read-only panel describing the current state of DHCP clients currently using the service. The Lease Info panel contains the Customer LAN Lease Info.

Figure 135 Lease Info

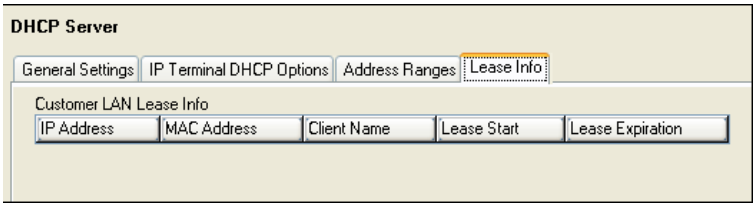


Table 107 Lease Info

Attribute	Value	Description
IP Address	<read-only>	The IP address currently supplied to the client.
MAC Address	<read-only>	The MAC address of the client.
Client Name	<read-only>	The client name, if the client was given a name in the Reserved Addresses table. Otherwise, this field is blank.
Client Description	<read-only >	Specify the description that will help to identify the client to which this IP address is assigned.
Lease Start	<read-only date format: yyyy-mm-dd hh:mm:ss>	The date and time the lease began.
Lease Expiration	<read-only date format: yyyy-mm-dd hh:mm:ss>	The date and time the lease is set to expire.

Chapter 67
DHCP configuration with router

If you have a BCM with an embedded router (BCM50a or BCM50e), the BCM requests its IP configuration from the router. By default, the IP address of the integrated router is 192.168.1.1. By default it always reserves 192.168.1.2 for the BCM LAN. If the IP address of the router is changed, the IP address of the BCM LAN also changes.

Changing the default router DHCP configuration

The DHCP Server also supplies the Nortel specific information that are required by IP sets. This information includes TPS server information and VLAN ids. If the S1 and S2 IP addresses are left as their default, they will automatically be updated when the router's IP address is changed. If the S1 and S2 addresses have been entered manually, they will not be automatically updated when the router's IP address is changed.

Configuring the BCM with a DHCP address

To configure the BCM with a DHCP address

1. Set up your DHCP server, if it is not already configured on your network. If you are using a BCM with a router, consult the router documentation for information on configuring the DHCP network.
2. Connect the BCM to the network. By default, the BCM will detect the presence of a DHCP server, and set itself up as a client of this DHCP server.

Configuring the BCM to act as a DHCP server

The BCM needs to act as a DHCP server only if there is no integrated router. By default, the BCM will attempt to detect the presence of another DHCP server, and determine whether it needs to offer DHCP services.

To configure the BCM DHCP component

1. Determine the status of the DHCP server. In most scenarios, you can leave it as automatic.
2. Configure the IP address range and DNS information.
3. Configure the proxy server settings.

Determining the status for the DHCP server

By default, the DHCP server on the BCM is set to **enabled-automatic**. This means that it will automatically detect whether there is already a DHCP server on the network. This feature covers all of the following scenarios:

- The network is already using DHCP from another server, but the network contains devices that require the BCM DHCP server, such as Nortel IP Phones.
- The network is already using DHCP from another server, and the network does not contain any devices that require the BCM DHCP server.
- The network does not have a DHCP server, and the BCM DHCP server is required to provide IP addresses to all DHCP clients.

If your network matches one of these configuration scenarios, ensure that the DHCP status is set to **enabled-automatic**.

If the network configuration does not match any of these scenarios, you can either disable the DHCP server, set the DHCP server to respond to requests from IP phones only, or set the DHCP server to respond to requests from all DHCP clients.

Using the BCM as a standalone DHCP server

If there is no DHCP server on the network, the BCM will use the following as a default IP configuration:

- IP Address: 192.168.1.2
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1

The DHCP server on the BCM will provide all necessary information to DHCP clients on the networks.

DHCP for IP sets

In addition to IP address information, IP sets require additional information if they are set to Full DHCP mode. This information includes the IP address, port number, action, and retry count for both the primary and secondary terminal proxy server.

Disabling the DHCP server

To disable the DHCP server

1 Click **Configuration > Telephony > Data Services > DHCP Server > General Settings** tab.

2 Select **Disabled** from the **DHCP server is** list.

Chapter 68
Firewall configuration resources

Table 108 shows the port configurations that must be allowed on a firewall for the BCM to function properly.

Table 108 Firewall configuration

Port	Type	Description
5989	TCP	Required for running Element Manager across a firewall
25	TCP	SMTP used for Unified Messaging
143	TCP	IMAP used for Unified Messaging
161	UDP	SNMP management
162	UDP	SNMP traps
389	TCP	LDAP used for Unified Messaging
1222	TCP	LAN CTE client traffic
1718	TCP	H.323 signaling traffic
1719	TCP	H.323 signaling traffic
1720	TCP	H.323 signaling traffic
5000	UDP	QoS monitor probe packets
5060	UDP	SIP traffic
7000	UDP	Unistim IP set signaling traffic
20000-20255	UDP	Voice Path for IP telephony which is used when 28000 range is unavailable
28000-28255	UDP	Voice Path for IP trunks

Chapter 69
Dial Up overview

The dial-out interfaces on the BCM offer three key services:

- **Remote Access** allows users at a client station to connect to the BCM across a phone line using Point to Point Protocol (PPP). This allows a person working from home or from a remote location to connect to the BCM LAN through a modem and a phone line.
- **Automatic Dial-Out** automatically establish a PPP connection to a remote location through a phone line. Automatic Dial-out can be used for services such as SNMP Trap delivery service, Log download, Backup download, CDR records push, Software Updates pulls and the Key Codes file upload.
- **WAN Failover** is used in conjunction with the Integrated Router. The Integrated Router monitors the status of the primary WAN link. When the primary WAN link is detected to have failed, the Integrated Router will route the traffic to the WAN Failover dial-up interface. When the WAN link recovers the dialled failover WAN connection is terminated and the IP traffic is then routed over the primary WAN link.

The primary WAN link is located on the integrated router and the dialup links are located on the CSC card.

Refer to the following information on Remote Access, Automatic Dial-Out, and WAN failover services:

- “Remote Access Service” on page 498
- “Automatic Data Dial-Out Service” on page 499
- To configure Dial-In:

  “Modem Dial-In Parameters panel” on page 514

  “ISDN Dial-In Parameters panel” on page 518
- To configure Dial-Out:

  “Dial-out Interfaces panel” on page 501
- To configure WAN failover

  “WAN failover” on page 513

Remote Access Service

Remote Access Service (RAS) allows a client system to dial a telephone number and establish an IP link with a BCM. This link is a connection across a telephone network over an ISDN line, or between a modem on the client system and a modem on the BCM. Once this link is established, the client can run IP applications to access the BCM system's OAM server, Web Page Server or BCM Monitor.

A user must provide credentials to establish the PPP connection. The credentials used must match the ones of a BCM account which has the PPPLogin privilege.

Note: The modem or ISDN interface must be enabled for a connection to take place.

The BCM can be configured with callback users along with their callback numbers. In this scenario, the user can ask BCM to callback before establishing the PPP connection. The BCM will validate the user name and use the callback number associated with the account where the user name was found. The authentication will be made using the user name and password associated with the account where the callback user name was found. The modem will try to call a configurable amount of time, with a configurable delay between attempts.

The BCM modem or ISDN interface will automatically disconnect if there is no traffic on the IP link for a configurable amount of time.

The IP addresses assigned to the BCM and the remote client are configurable.

- The default configuration for the modem dial-in is for the BCM to assign itself an address of 10.10.14.1 and assign to the remote client an address of 10.10.14.2. The settings can be changed to have the remote client assign itself an address or even assign the BCM an address.
- The default configuration for ISDN dial-in is for the BCM to assign the first ISDN interface an address of 10.10.18.1 and the second client an address of 10.10.18.2. The first remote client is assigned 10.10.18.10 and the second client is assigned 10.10.18.11. The settings can be changed to have the remote clients assign themselves an address or even assign the BCM an address.

Finally, an administrator has the capability to disconnect a modem or ISDN call if they find that a modem or ISDN call is in progress.

To program the RAS configurable options, select:

- **Configuration > Resources> Dial Up Interfaces > Modem Dial-In Parameters**
- **Configuration > Resources> Dial Up Interfaces > ISDN Dial-In Parameters**

Modem Remote Access Service Specifics

For Modem dial in, the Auto-disable feature will automatically disable the modem if no connections are established for a configurable period of time. The Auto-disable feature is turned off by default. The modem can be enabled through Element Manager, using Feature 9*8 or the Startup Profile. If the modem is enabled using the Startup Profile, the Auto-disable capability is turned off.

The modem has a Directory Number (DN) associated with it. This DN can be used to redirect a call to the modem. A call can be redirected to the modem DN using the F70 (Transfer) feature from any sets attached to the BCM, or it can be redirected to the modem DN using the Auto-Attendant feature. Any user on the BCM can redirect an active call at their set by using Feature 9*0 if they don't know the modem DN. Feature 9*0 will also display the modem DN on any sets with at least 1 line display.

The modem can also be programmed to answer incoming lines directly after a configurable number of rings. Please be aware that most modems are programmed by default to give up on a connection after 60 seconds. If the number of rings and the amount of time it takes for the 2 modems to establish a connection take more than 60 seconds, the connection will fail. If an administrator wants a modem to answer after a longer period than this default timeout, the calling modem answer timeout should be changed accordingly.

Internal calls to the modem will always be answered immediately. External calls transferred to the modem will be answered after the number of rings specified on the Modem Dial-In Parameters tab. This gives enough time to wait and collect caller ID information which will be captured and logged every time the modem connects.

Automatic Data Dial-Out Service

Automatic Dial-Out Service allows IP communications with a remote server through the modem or ISDN interface.

The user can configure the BCM system to automatically set up a modem or ISDN connection with a remote PPP server for establishing a PPP link when it needs to deliver IP data packets. Many services on the BCM have destination or source addresses which could be resolved by a route associated with the Auto Dial-Out service. The SNMP Trap delivery service, Log download, Backup download, CDR records push, Software Updates pulls, and the Keycodes file upload are just examples of such services. An administrator must be aware that the use of scheduled services over the modem may not give the expected results as a modem connection could fail for many different reasons and besides the SNMP v3 trap delivery, those services have no retry capabilities.

The triggering IP data follows a configured IP route to access the PPP interface, which then activates a dialing script to cause the modem to dial a remote number, starts PPP negotiation, establishes PPP link, and delivers the data packets.

After a configurable period of inactivity over the PPP link, the modem or ISDN link is disconnected. Any new IP data packets will then trigger the connection again. Please keep in mind the long distance charges when configuring the inactivity timeout. Sometimes it is cheaper to keep a link up a bit longer than to make two calls of shorter periods.

The number to dial has to be a number which can be dialed using a Destination Code (route). The modem or ISDN link cannot use a Line Pool access code to dial out.

The BCM will use the user name and password associated with the configured account to authenticate itself with the remote server.

The IP addresses assigned to the BCM and the remote server are configurable. Both must be resolvable with the routes programmed for dialing out and the remote server address must match the address supplied when programming the service that will attempt to deliver the packets. More than one route can be programmed, but all will use the same phone number to reach the remote server.

To program the Automatic Data Dial-Out configurable options in Element Manager, select **Configuration > Resources > Dial Up Interfaces > Dial-Out Interfaces**.

WAN Failover Service

The WAN failover service is used in conjunction with the Integrated Router. The Integrated Router monitors the status of the primary WAN link. When the primary WAN link is detected to have failed, the Integrated Router will route the traffic to the WAN Failover dial-up interface, if one is configured. The dial-up interface can be ISDN or an analog modem. When the WAN link recovers the dialed failover WAN connection is terminated and the IP traffic is then routed over the primary WAN link.

The WAN Failover Interface can be programmed in Element Manager:

Configuration > Resources > Dial Up Interfaces > Global Settings

Note: Dial-out interfaces to be used as the Failover Interface must not be provisioned for an automatic dialout service.

Modem compatibility

The internal modem is compatible with all V.34 modems, and has been tested with the following modems:

- U.S. Robotics Sportster 33.6 FaxModem (external modem)
- Microcom DeskPorte 28.8P (external modem)
- PCTEL 2304WT V.92 MDC (internal modem Dell Portable)
- U.S. Robotics Sportster 56K (external modem)

Chapter 70
Dial Up Interfaces panel

The Dial Up Interfaces panel contains four sub-panels:

Panel	Task
Dial-out Interfaces panel	Add and configure the dial-out interfaces
Global Settings panel	Set the WAN Failover interface
Modem Dial-In Parameters panel	Configure and check the status of the modem dial-in interface
ISDN Dial-In Parameters panel	Configure and check the status of the ISDN dial-in interfaces

Dial-out Interfaces panel

On the Dial-out Interfaces panel you can add, configure, and control the connection status of both ISDN and Modem dial-out interfaces. These interfaces can be used for either Automatic dial-out service or WAN Failover Service.

ISDN configuration

- “ISDN interfaces” on page 502
- “ISDN Dial-out Channel Characteristics” on page 505
- “ISDN Dial-out Link Parameters” on page 506
- “ISDN Dial-out IP Address” on page 508

Modem configuration

- “Modem interface” on page 508
- “Modem Dial-out Link Parameters” on page 510
- “Modem Dial-out IP Address” on page 512

Figure 136 Dial-out Interfaces panel

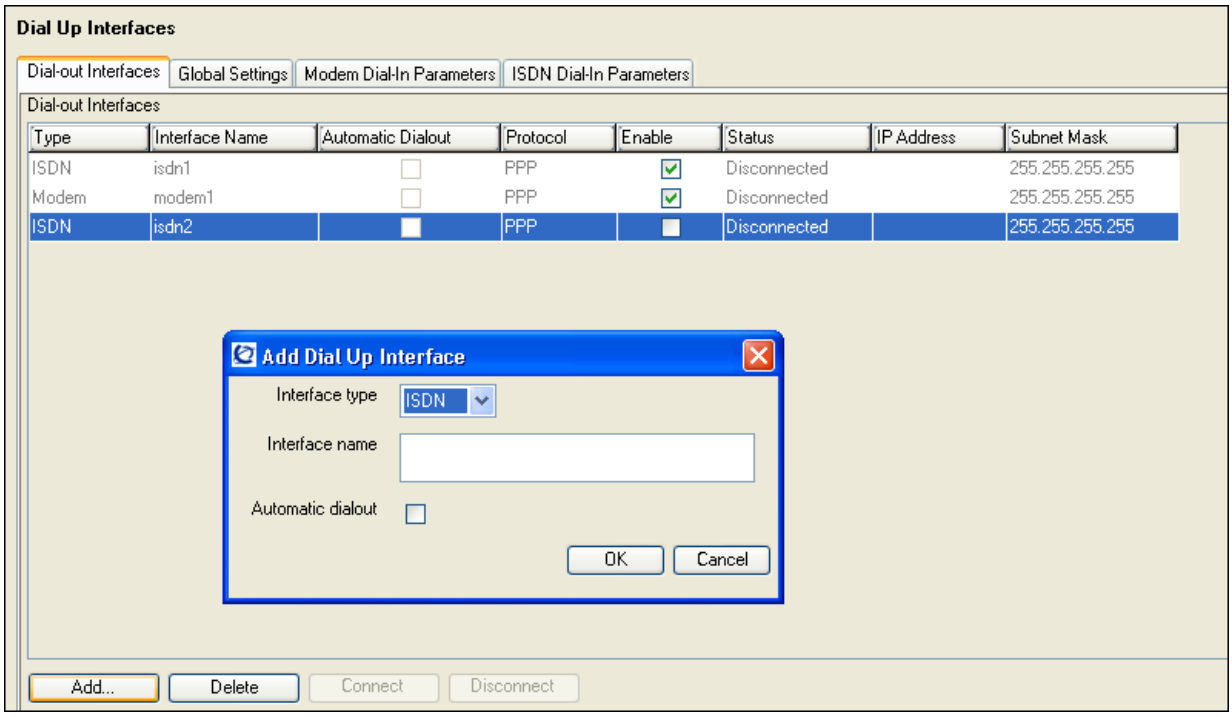


Table 109 Dial-out Interfaces fields

Attribute	Value	Description
Type	<drop-down list>	Select the type of interface to be added. Interface types supported: Modem, ISDN
Interface Name	<alphanumeric string>	Enter a logical name to identify the interface.
Automatic dialout	<check box>	Enable or disable the interface for Automatic dialout. Selected: static routes can be added for this interface. Cleared: this interface can be used for WAN Failover. **Note**: Automatic dial-out interfaces can not be used for WAN failover.
Protocol	<read-only>	Always PPP.
Enable	<check box>	Enable or disable the interface.
Status	<read-only>	Current connection status: Disconnected, Connecting, Connected.
IP Address	<read-only>	IP address assigned to the connected interface.
Subnet Mask	<read-only>	Subnet mask assigned to the connected interface.

ISDN interfaces

ISDN interfaces can only be configured on a BCM50 with an integrated BRI module, or on a BCM with a BRI MBM installed in the expansion unit. A maximum of two BRI-ISDN interfaces are supported on each BCM. Each of these interfaces supports two ISDN B-channels.

To add an ISDN interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, click **Add**.
The **Add Dial Up Interface** dialog box appears.

3 Select **ISDN** from the **Interface type** drop-down list.

4 Enter a logical name in the **Interface name** field.

5 Select the **Automatic Dialout** check box to use this interface for scheduled service. Refer to "Creating an automatic dial-out interface" on page 521.

6 Click **OK**.
The interface appears in the Dial-out Interfaces table.

Enabling an ISDN interface

An interface must be enabled to function as a backup connection. If the BCM experiences a primary connection failure, it will dial-out using the dial-up interface configured as the backup. See "WAN failover" on page 513.

To enable an ISDN interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, select the ISDN interface.

3 On the **Link Parameters** tab, enter the **Dial-out number** for the ISDN interface.

4 On the **Dial-out Interfaces** tab, select the **Enable** check box next to the ISDN interface to enable.

Note: BCM50 R2 will only allow the configuration of two ISDN auto-dialout interfaces. When both of these interfaces are enabled ISDN dial-in will be disabled.

To disable an ISDN interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, clear the **Enable** check box next to the interface.

Connecting an ISDN interface

Interfaces can be connected manually, or they can be triggered to connect by auto dial-out, see "Creating an automatic dial-out interface" on page 521. Auto dial-out routes can not be added if the interface is already manually connected, unless the interface is already connected with auto dial-out routes configured.

To manually connect an ISDN interface

1. Click **Configuration > Resources > Dial Up Interfaces**.
2. On the **Dial-out Interfaces** tab, select the interface to connect.
3. Select the **Enable** check box.
4. In the **IP Address Specification** tab, specify the remote IP address to which to connect.
5. In the top panel, click **Connect**.

To disconnect an ISDN interface

1. Click **Configuration > Resources > Dial Up Interfaces**.
2. On the **Dial-out Interfaces** tab, select the interface to disconnect.
3. Click **Disconnect**.
   A confirmation dialog box will appear.
4. Click **Yes**.

To delete an ISDN interface

1. Click **Configuration > Resources > Dial Up Interfaces**.
2. Clear the **Enable** check box.
3. Click the ISDN interface you want to delete.
4. Click **Delete**.
5. Click **Yes**.
   The interface is deleted.

ISDN Dial-out Channel Characteristics

Figure 137 ISDN Dial-out Interface Channel Characteristics tab

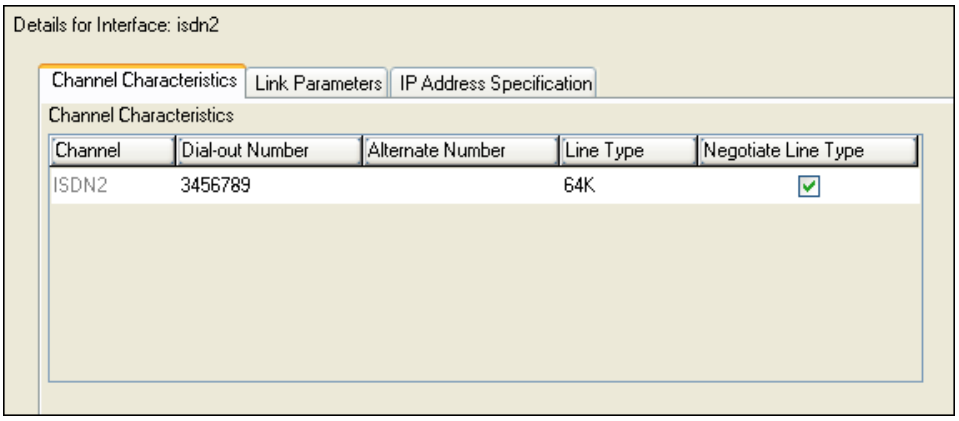


Table 110 ISDN Dial-out Interface Channel Characteristics fields

Attribute	Value	Description
Channel	<read-only>	There are two ISDN channels available for dial out, ISDN1 and ISDN2. These channels are assigned automatically.
Dial-out Number	<numeric string>	Enter the primary phone number to use to make an ISDN connection. If needed, include area codes and all necessary digits to dial an external number. The phone number must contain only numerical digits (no alphabetical or other characters are allowed). Default: blank
Alternate Number	<numeric string>	Alternate phone number if the Primary Phone number is unreachable. Default: blank
Line Type	<drop-down list>	Select either 64K Digital or 56K Digital line. BCM ISDN supports two types of Unrestricted Digital Information (UDI) bit streams: UDI, and UDI-56. With UDI, data is transmitted at 64kbps (64K Digital). With UDI-56, a 1 bit is inserted in the eighth bit position of each B-channel time slot while the other 7 bits form the 56kbps channel (56K Digital). Default: 64K Digital
Negotiate Line Type	<check box>	Select whether the system will select a line with a slower speed if unable to connect at the previously set speed. Default: enabled

To modify the characteristics of an existing ISDN channel

1. Click **Configuration > Resources > Dial Up Interfaces**.
2. Click the ISDN interface to configure.
3. Select the **Channel Characteristics** tab.
4. Double-click the field to modify.
5. Make the necessary changes.

ISDN Dial-out Link Parameters

Figure 138 ISDN Dial-out Interface Link Parameters tab

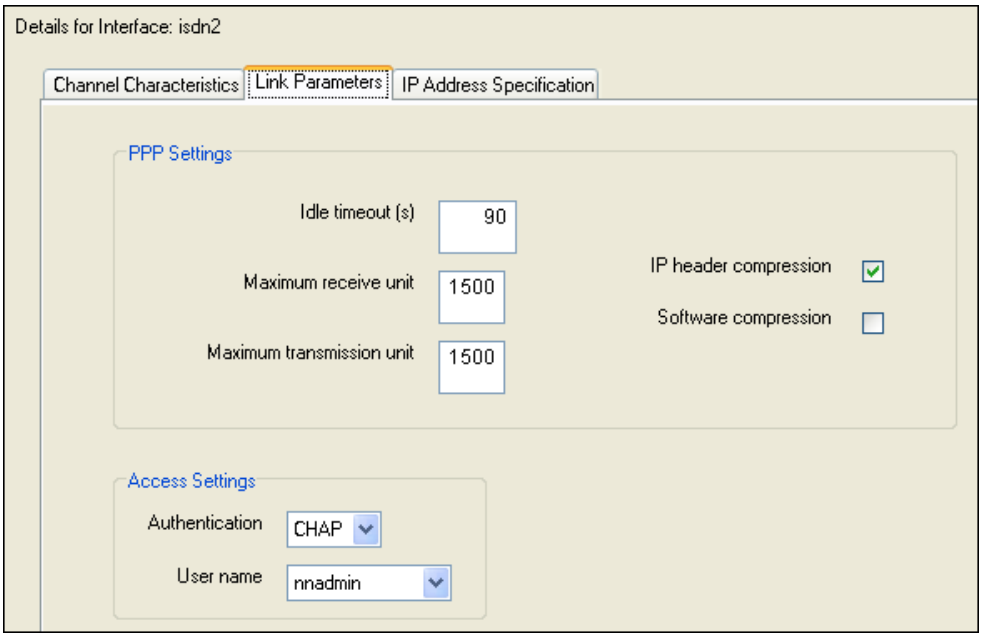


Table 111 ISDN Dial-out Interface Link Parameters fields (Sheet 1 of 2)

Attribute	Value	Description
PPP Settings		
Idle Timeout (s)	<0–36000>	The interval after which the ISDN interface disconnects when there is no traffic. Default: 90 seconds **Note**: A value of 0 makes the connection persistent.
Maximum Receive Unit	<128–1500>	The maximum size of the packets that can be received. Default: 1500
Maximum Transmit Unit	<128–1500>	The maximum size of the packets that can be sent. Default: 1500

Table 111 ISDN Dial-out Interface Link Parameters fields (Sheet 2 of 2)

Attribute	Value	Description
IP Header Compression	<check box>	Enable or disable IP header compression. **Note**: The feature must be enabled at both ends of the connection. Default: enabled
Software Compression	<check box>	Enable or disable software compression. When enabled, all dial-up connections use BSD Scheme for compression. Default: disabled
Access Settings		
Authentication	PAP or CHAP	Select the authentication type for the link. Default: CHAP
Dial-Out User Name	<drop-down list>	Enter the username used for authenticating to the remote end.

To configure the ISDN Link Parameters

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 Click the ISDN interface to configure.

3 Click the **Link Parameters** tab.
The Link Parameters panel appears. See Figure 138.

4 Configure the ISDN Link Parameters. Refer to the information in Table 111.

ISDN Dial-out IP Address

Figure 139 ISDN Dial-out Interfaces IP Address Specification tab

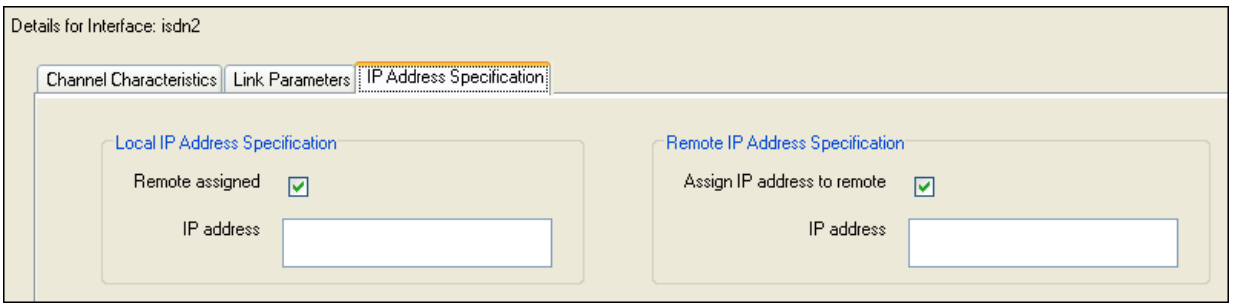


Table 112 ISDN Dial-out Interfaces IP Address Specification fields

Attribute	Value	Description
Local IP Address Specification		
Remote assigned	<check box>	When selected, the BCM obtains its IP address from the remote end. Default: selected
IP address	<IP Address>	When the Remote Assigned parameter is disabled, a static IP address must be configured in this parameter.
Remote IP Address Specification		
Assign an IP address to remote	<check box>	When selected, BCM will assign the IP address in the “IP Address” field of this section to the remote end of the connection. Default: cleared
IP address	<IP Address>	The local IP address used on the BCM for the dial-out connection. Default: 10.11.16.1

Modem interface

BCM supports one V.34 modem connection to, and from, the BCM50.

Caution: Do not modify any of the advanced modem settings on the integrated router.

To add the modem interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, click **Add**.
The **Add Dial Up Interface** dialog box appears.

3 Select **Modem** from the **Interface type** drop-down list.

4 Enter a logical name in the **Interface name** field.

5 Select the Automatic dialout check box to use this interface for scheduled service. Refer to "Creating an automatic dial-out interface" on page 521.

6 Click **OK**.
The interface appears in the Dial-out Interfaces table.

Enabling the modem interface

An interface must be enabled to function as a backup connection. If the BCM experiences a primary connection failure, it will dial-out using the dial-up interface configured as the backup. See "WAN failover" on page 513.

To enable the modem interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, select the modem.

3 On the **Link Parameters** tab, enter the **Dial-out number** for the modem.

4 On the **Dial-out Interfaces** table, select the **Enable** check box for the modem
The interface is now enabled.

To disable the modem interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, select the modem to disable.

3 On the Dial-out Interfaces tab, clear the **Enable** check box next to the modem.

Connecting a modem interface

Interfaces can be connected manually, or they can be triggered to connect by auto dial-out, see "Creating an automatic dial-out interface" on page 521. Auto dial-out routes can not be added if the interface is already manually connected, unless the interface is already connected with auto dial-out routes configured.

To manually connect the modem interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, select the interface to connect.

3 Select the **Enable** check box.

4 In the **IP Address Specification** tab, specify the remote IP address to which to connect.

5 In the top panel, click **Connect**.

To disconnect a modem interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 On the **Dial-out Interfaces** tab, select the interface to disconnect.

3 Click **Disconnect**.
A confirmation dialog box will appear.

4 Click **Yes**.

To delete a modem interface

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 Clear the **Enable** check box.

3 Click the modem interface.

4 Click **Delete**.
A confirmation dialog box appears.

5 Click **Yes**.
The interface is deleted.

Modem Dial-out Link Parameters

Figure 140 Modem Dial-out interface Link Parameters tab

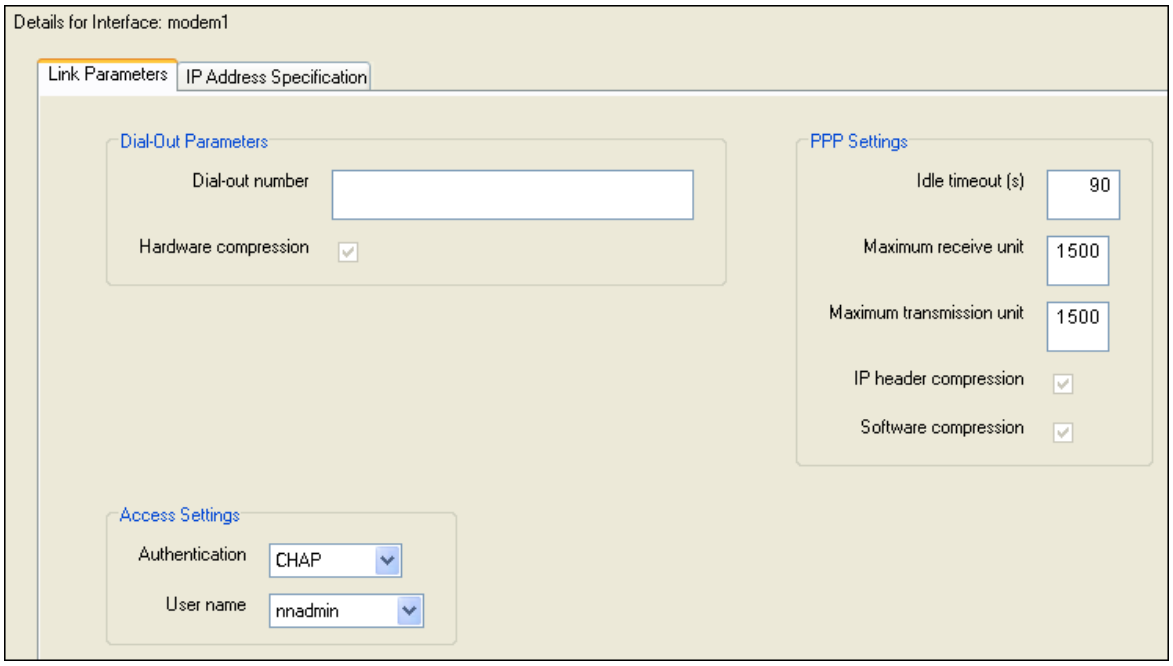


Table 113 Modem Dial-out Interface Link Parameters fields

Attribute	Value	Description
Dial-Out Parameters		
Dial-out number	<numeric string>	Telephone number to use to connect using the modem interface. If needed, area codes and all necessary digits to dial an external number are included.
Hardware Compression	<read-only>	Hardware compression is always enabled.
PPP Settings		
Idle timeout	<90–36000>	The interval after which the modem interface disconnects when there is no traffic. Default: 90 seconds **Note**: Specifying a value of 0 makes the connection persistent.
Maximum Receive Unit	<128-1500>	The maximum size of the packets that can be received. Default: 1500
Maximum Transmit Unit	<128-1500>	The maximum size of the packets that can be sent Default: 1500
IP Header Compression	<read-only>	IP header compression is always enabled.
Software Compression	<read-only>	Software compression is always enabled.
Access Settings		
Authentication	PAP CHAP MSCHAP MSCHAPv2	The authentication type for the link. Default: CHAP
User name	<drop-down list>	Username that the link uses to authenticate itself when dialling out to another router. Default: nnadmin

To configure the Modem Link Parameters

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 Click the Modem interface to configure.

3 Click the **Link Parameters** tab.
The Link Parameters panel appears. See Figure 140.

4 Configure the Modem Link Parameters. Refer to the information in Table 113.

Modem Dial-out IP Address

Figure 141 Modem Dial-out Interface IP Address Specification tab

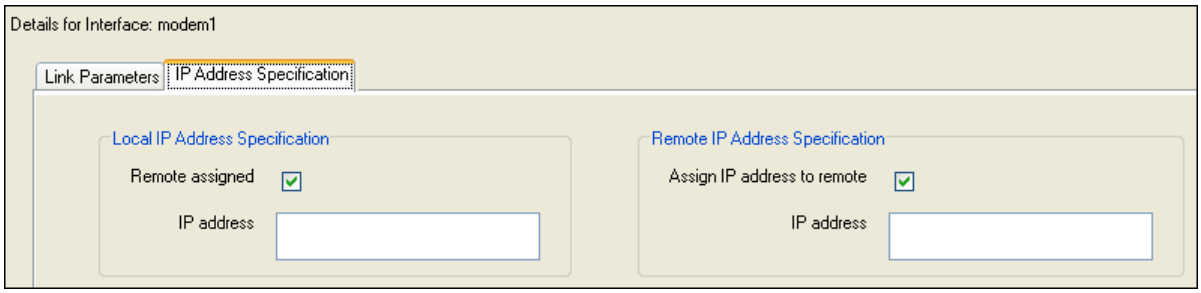


Table 114 Modem Dial-out Interface IP Address Specification fields

Attribute	Value	Description
Local IP Address Specification		
Remote Assigned	<check box>	When selected, the BCM obtains it's IP address from the remote end. Default: enabled
IP address	<IP Address>	When the Remote Assigned parameter is disabled, a static IP address must be configured in this parameter.
Remote IP Address Specification		
Assign IP address to remote	<check box>	When selected, BCM will assign the "IP Address" field of this section to the remote end of the connection.
IP Address	<IP Address>	The local IP address used on the BCM for the dial-out connection. Default: 10.11.16.16

To configure the Modem IP Address Specification

1. Click **Configuration > Resources > Dial Up Interfaces**.
2. Click the Modem interface to configure.
3. Click the **IP Address Specification** tab.
   The IP Address Specification panel appears. See Figure 141.
4. Configure the IP Address Parameters. Refer to the information in Table 114.

Global Settings panel

The Global Settings panel contains the specification of the Failover Interface. This is a drop-down list of the Dial-out interfaces that do not have "Automatic dial-out" selected. Refer to "WAN failover" on page 513. The Global settings panel is shown in Figure 142.

Figure 142 Global Settings panel

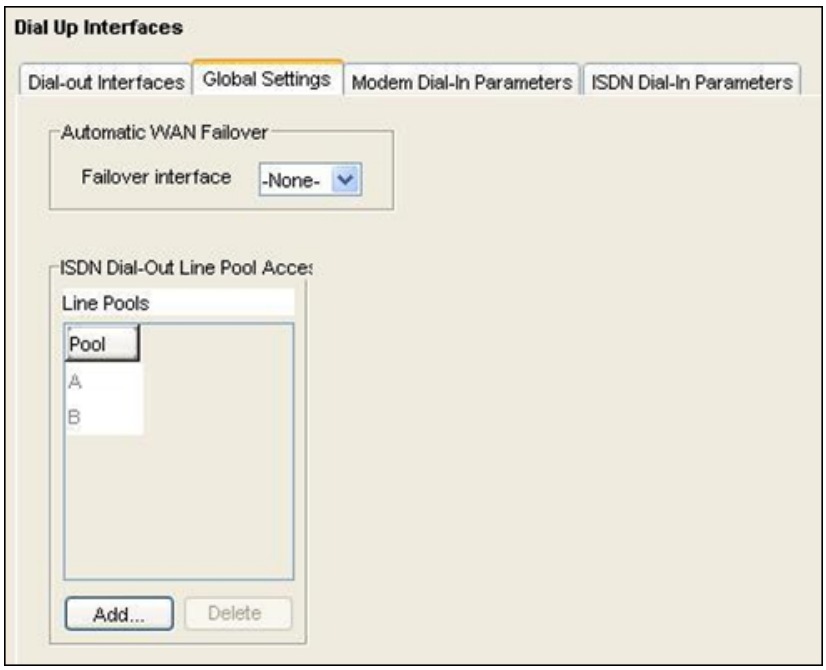


Table 115 Global Settings field

Attribute	Value	Description
Automatic WAN Failover		
Failover interface	<drop-down list>	Select one of the existing dial-out interfaces that is not selected for “Automatic dialout”. Dial-out interfaces are provisioned from the Dial-out Interfaces tab in this same section. Default: -None- **Note:** This parameter will not be displayed if the particular BCM does not have the hardware to provide Failover support.
ISDN Dial-Out Line Pool Access		Assign a Line Pool for ISDN dial out.

WAN failover

The Integrated Router monitors the status of the primary WAN link. When the primary WAN link is detected to have failed, the Integrated Router will route the traffic to the WAN Failover dial-up interface, if one is configured. Refer to “WAN Failover Service” on page 500.

Caution: Router Settings

The following settings must be configured on the router for WAN failover to function:

Port Speed - 115200
Enable Dial Back-Up check box - selected

Do not change any other Basic or Advanced router settings.

Note: The WAN failover feature operates only on BCM50a, BCM50e, BCM50ba, or BCM50be Release 2.

To assign a modem interface for WAN failover

1. Create, and enable, a modem interface. See "To add the modem interface" on page 508.
2. Click **Configuration > Resources > Dial Up Interfaces > Global Settings**.
3. From the **Failover interface** drop-down list, select the interface to configure as a WAN backup.

To assign an ISDN interface for WAN failover

1. Create, and enable, an ISDN interface. See "To add an ISDN interface" on page 503.
2. Click **Configuration > Resources > Dial Up Interfaces > Global Settings**.
3. From the **Failover interface** drop-down list, select the interface to configure as a WAN backup.
4. Click Add on the **ISDN Dial-Out Line Pool Access** subpanel.
   The **Add Line Pool** dialog box appears.
5. Enter a line pool the ISDN interface can use to dial out.
6. Click **OK**.

Modem Dial-In Parameters panel

The Modem Dial-In parameters controls Dial-in to the BCM for remote access. This panel is used to configure the modem for Dial-in. It also displays the connection status of the modem if one is in progress. The Modem Dial-in Parameters panel is shown in Figure 143. If the BCM50 has an integrated router (BCM50a or BCM50e), see "Additional configuration to allow network access functionality" on page 517.

Figure 143 Modem Dial-In Parameters panel

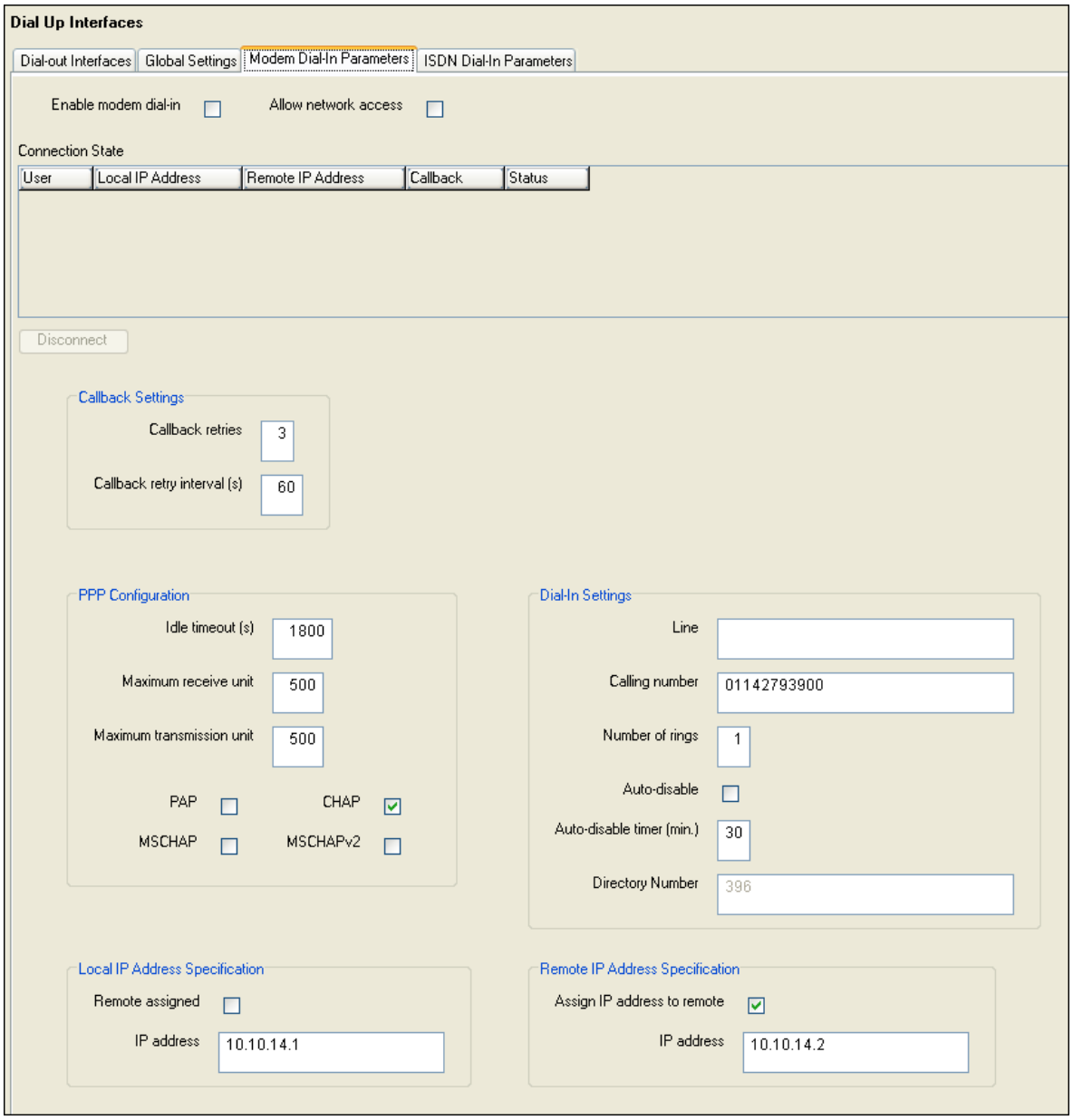


Table 116 Modem Dial-In Parameters fields (Sheet 1 of 3)

Attribute	Value	Description
Enable Modem Dial-In	<check box>	Enable or disable modem dial-in. Default: disabled
Allow network access	<check box>	Enable or disable dial-in access to the entire network. Default: disabled
Connection State: This is a table that shows the current dial in state if connected. **Note**: There is a maximum of one entry in this table (as there is only one modem). This table will be blank if no dial in connection is currently active.		

Table 116 Modem Dial-In Parameters fields (Sheet 2 of 3)

Attribute	Value	Description
User	<read-only>	Displays the user that is currently dialed in.
Local IP Address	<read-only>	The local IP address assigned to the dial-in connection.
Remote IP Address	<read-only>	The remote IP address of the dial-in connection.
Callback	<read-only>	Displays if callback is enabled for this dial-in connection.
Status	<read-only>	The status of the dial-in connection.
Callback Settings		
Callback retries	<1-10>	The number of attempts made by the BCM to dial-out to the remote end during callback. Default: 3
Callback retry interval (s)	<0-360>	Interval for successive connection attempts for dial-out during callback. Default: 60 seconds
PPP Configuration. These parameters are passed to PPP stack to manage the PPP connection.		
Idle timeout	<numeric string>	Idle time after which, PPP will terminate the PPP connection. Default: 1800 seconds
Maximum Receive Unit	<128–1500>	The maximum size of the packets that can be received. Default: 500
Maximum Transmit Unit	<128–1500>	The maximum size of the packets that can be sent. Default: 500
Authentication support	PAP CHAP MSCHAP MSCHAPv2	Supported PPP authentication Default: CHAP
Dial-In Settings		
Line	<numeric string>	Line number monitored by the modem for incoming calls. A value of 0 = blank. Range: Min Target Line-Max Target Line Default: blank
Calling Number	<numeric string>	Analog modem uses this Calling Number (Calling ID – CLID) to detect an incoming data call.
Number of Rings	<1-10>	Number of rings before the BCM redirects a call to the modem. This field applies only when a call is directed to the line number specified in this section. Otherwise, this value is ignored and the modem answers 10 seconds after a call is presented. **Note**: The number of rings, for certain market profiles, must be multiplied by 2 due to double ring cadence. For these profiles, the maximum number of rings is 5. (5x2=10) Default: 1
Auto-disable	<check box>	When selected, the modem is automatically disabled after use. Default: disabled

Table 116 Modem Dial-In Parameters fields (Sheet 3 of 3)

Attribute	Value	Description
Auto-disable timer	<0-30 minutes>	Time after which the Dial-in for the modem is disabled after use. Default: 0
Directory Number	<read-only>	Read-only number assigned to the analog modem. Used for manual transfer of call or by auto-attendant.
Local IP Address Specification		
Remote assigned	<check box>	If selected, the BCM obtains its IP address from the remote end. Default: disabled
IP Address	<IP Address>	Use this IP Address as the local IP address for the PPP connection. This value is used when “Remote assigned” is disabled. Default: 10.10.14.1
Remote IP Address Specification		
Assign IP address to remote	<check box>	If selected, the BCM will assign the IP address specified in the **IP Address** field of this section to the remote end of the connection. Default: selected
IP Address	<IP Address>	When the **Assign IP address to remote** is enabled BCM will assign to the remote end of the connection the IP address specified in this field. Default: 10.10.14.2

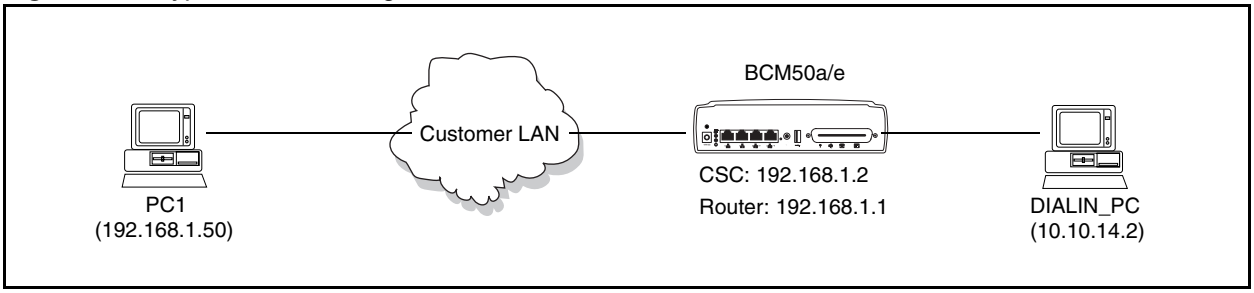
Additional configuration to allow network access functionality

If the BCM50 has an integrated router (BCM50a or BCM50e), then you must:

- Configure a static route on the integrated router.
- Configure the firewall on the integrated router to Bypass Triangle Route.

For example, consider the network configuration shown in Figure 144.

Figure 144 Typical dial-in configuration



If you want DIALIN_PC to access PC1 (192.168.1.50) on the customer LAN, then you must configure a static route on the integrated router to route all traffic for the dial-in IP address to the CSC card on the BCM50 (192.168.1.2). The static route is configured as shown in Table 117:

Table 117 Static route configuration

Parameter	Value
Active	Selected
Destination IP Address	10.10.14.0
IP Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Metric	1

You must also configure the firewall on the integrated router to Bypass Triangle Route. Using the same example, if there is a ping request from DIALIN_PC (10.10.14.2) to PC1 (192.168.1.50):

- The CSC receives the ping request at 10.10.14.1 and forwards the packet through the customer LAN (192.168.1.2) to PC1 (192.168.1.50).
- PC1 sends the ping reply to the integrated router (192.168.1.2) since this is the default gateway for PC1. PC1 does not have a route to 10.10.14.2.
- If Bypass Triangle Route is not selected, the firewall blocks the ping reply and generates the error message: out-of-order ICMP. This occurs because the integrated router does not see the ping request. The ping request was sent directly from the CSC (192.168.1.2) to PC1 (192.168.1.50).

For more information about configuring static routes and configuring Bypass Triangle Route, see *BCM50a Integrated Router Configuration — Basics* (N0115790) or *BCM50e Integrated Router Configuration — Basics* (N0115788).

ISDN Dial-In Parameters panel

The ISDN Dial-In Parameters controls Dial-in to the BCM for remote access. This panel is used to configure the ISDN for Dial-in. It also displays the connection status of the ISDN connections if any are in progress. Refer to Table 118 for a description of the ISDN Dial-in fields. If the BCM50 has an integrated router (BCM50a or BCM50e), see "Additional configuration to allow network access functionality" on page 517.

Note: ISDN Dial-in will be disabled if both ISDN auto-dialout interfaces are enabled.

Figure 145 ISDN Dial-in parameters fields

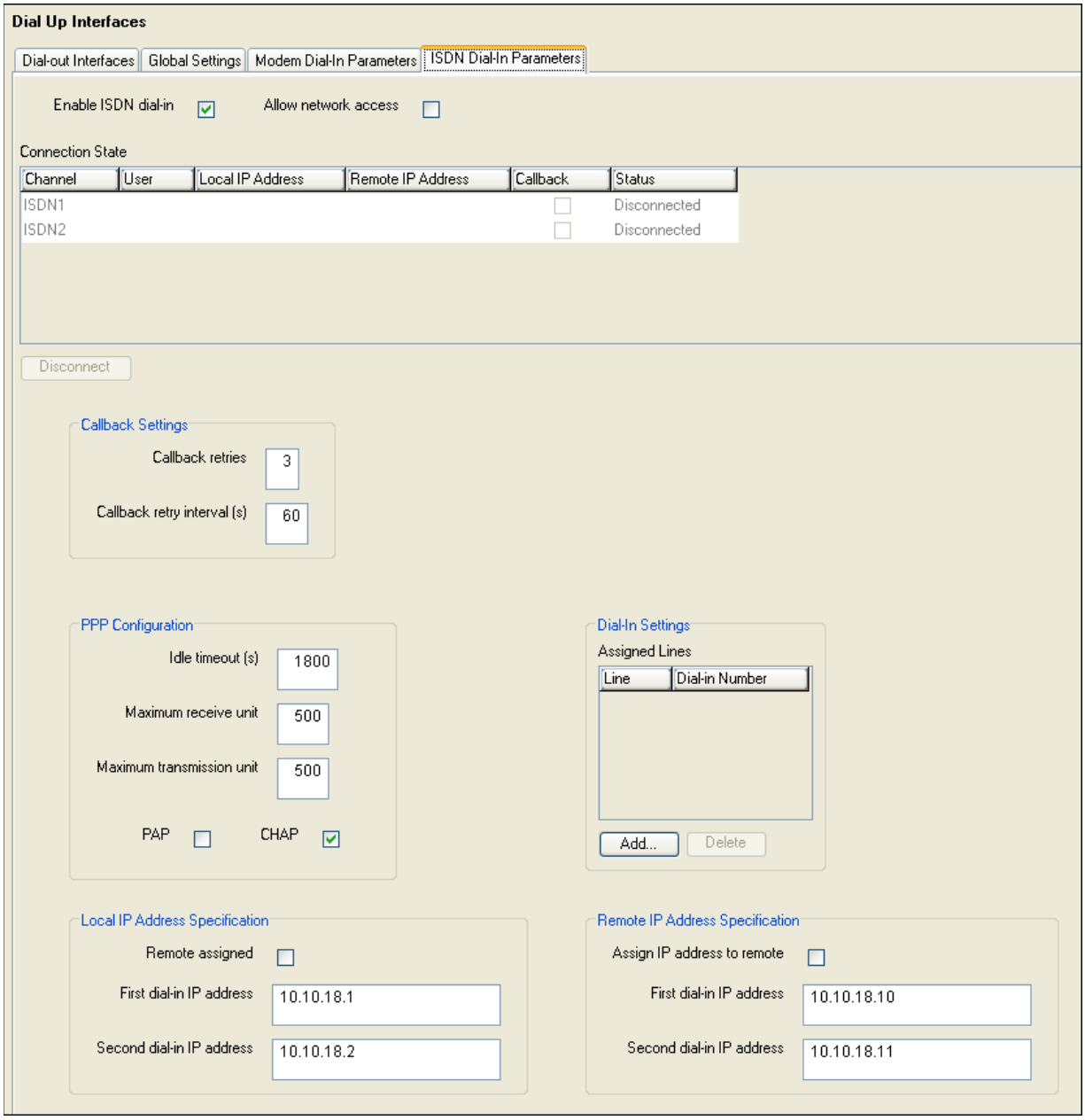


Table 118 ISDN Dial-In Parameters fields (Sheet 1 of 3)

Attribute	Value	Description
Enable ISDN dial-in	<check box>	Enable or disable ISDN dial-in. Default: disabled
Allow network access	<check box>	Enable or disable ISDN dial-in access to the entire network. Default: disabled

Table 118 ISDN Dial-In Parameters fields (Sheet 2 of 3)

Attribute	Value	Description
Connection State: This is a table that shows the current dial-in state if connected. **Note**: There is a maximum of two entries in this table (as there are two ISDN channels). This table will display the ISDN channels that are available for ISDN dial in. If any channels are being used for ISDN dial-out (either Automatic or manual) then this channel will not be available for ISDN dial-in, and will not appear in this table.		
Channel	<read-only>	The ISDN channel used.
User	<read-only>	Displays the user that is currently dialed in.
Local IP Address	<read-only>	Displays the local IP address assigned to the dial-in connection.
Remote IP Address	<read-only>	Displays the remote IP address of the dial-in connection.
Callback	<read-only>	Displays if callback is enabled for this dial-in connection.
Status	<read-only>	The status of the dial-in connection.
ISDN Callback Settings		
Callback retries	<1-10>	The number of attempts made by the BCM to dial-out to the remote end during callback. Default: 3
Callback retry interval (s)	<0-360>	Interval for successive connection attempts for dial-out during callback. Default: 60 seconds
PPP Configuration. These parameters are passed to PPP stack to manage the PPP connection.		
Idle timeout (s)	<numeric string>	Idle time period after which PPP will terminate the PPP connection. Default: 1800 seconds
Maximum receive unit	<128-1500>	The maximum size of the packets that can be received. Default: 500
Maximum Transmit Unit	<128-1500>	The maximum size of the packets that will be sent. Default: 500
Authentication support	PAP CHAP	Supported PPP authentication. Default: CHAP
Dial-In Settings		
Assigned Lines		Assign target lines for ISDN dial-in.
Local IP Address Specification		
Remote assigned	<check box>	When selected, BCM obtains its IP address from the remote end. Cleared, the BCM will use the addresses specified below for the first and second dial-in connections. Default: disabled
First dial-in IP Address	<IP Address>	The IP address that will be assigned to the BCM side of the first dial-in connection. This is only assigned if the **Remote Assigned** is disabled. Default: 10.10.18.1

Table 118 ISDN Dial-In Parameters fields (Sheet 3 of 3)

Attribute	Value	Description
Second dial-in IP Address	<IP Address>	The IP address that will be assigned to the BCM side of the second dial-in connection. This is only assigned if **Remote Assigned** is disabled. Default: 10.10.18.2
Remote IP Address Specification		
Assign IP address to remote	<check box>	When enabled, BCM will assign the remote end of the connection one of the IP addresses specified below. When cleared, the remote side will assign it's own IP address. Default: enabled
First dial-in IP Address	<IP Address>	The IP address that will be assigned to the remote side of the first dial-in connection. This is only assigned if **Assign IP address to remote** is enabled. Default: 10.10.18.10
Second dial-in IP Address	<IP Address>	The IP address that will be assigned to the remote side of the second dial-in connection. This is only assigned if **Assign IP address to remote** is enabled. Default: 10.10.18.11

Creating an automatic dial-out interface

Caution: Select the **Enable Dial Back-Up** check box to enable Dial Back-up on the router. Do not change the other Basic or Advanced Settings.

Management applications such as SNMP trap dial out, Scheduled Log transfer, Scheduled Backup, and Scheduled CDR records transfer can use automatic dial-out over an ISDN or Modem interface. To configure the automatic data transfer, the administrator must configure a static route, with the auto dial-out field selected, and associate it with the application. When data is sent to the destination address, the network recognizes the address of the application, and triggers the dial-out to establish the connection.The packets are then sent over the link to the destination.

Notes:

- The dial-out interface must be enabled to configure static routes.
- The disconnect time for the interface must be greater than 60 seconds. This is configured on the **Link Parameters** tab of the selected interface under **Configuration > Resources > Dial Up Interfaces**.
- Auto dial-out routes cannot be added if the interface is already manually connected, unless the interface is already connected with auto dial-out routes configured.

To add an automatic dial-out interface

1 Create a Modem or ISDN interface. See "To add an ISDN interface" on page 503 or "To add the modem interface" on page 508.

Note: If an interface is enabled and configured for manual dial-out, the interface must be disabled before it can be configured for automatic dial-out.

2 Enable the interface under **Configuration > Resources > Dial Up Interfaces**.

3 Select the **Automatic Dialout** check box for the interface.

4 Set the **Idle timeout (s)** on the **Link Parameters** tab to a value greater than 60 seconds.

5 Add a static route. Refer to "To add a new IP Static Route" on page 463.

6 Associate the route with an application.

To manually disconnect an auto dial-out interface

Note: Auto dial-out interfaces are disconnected automatically once data transfer is complete.

1 Click **Configuration > Resources > Dial Up Interfaces**.

2 Select the interface to disconnect.

3 Click **Disconnect**.
A confirmation dialog box will appear.

4 Click **Yes**.

Guidelines for using remote Dial-in

Consider the following guidelines when using remote dial-in:

- The remote dial-in for administration and the backup WAN link share the same modem. If a remote administration user is connected while the primary link breaks, the automatic backup function does not occur.
- While using the back-up interface, BCM always calls. BCM does not answer an incoming call from a router on the V.92 interface.

Using a dial-up interface as a primary connection

The dial-up interfaces on the BCM are used as a Primary or Secondary interfaces. The BCM does not have default dial-up settings, the Administrator must add them.

The following tasks can be configured to use dial-up as a primary connection:

- SNMP auto trap dial-out
- modem user secure callback
- CDR records retrieval
- backup to a remote destination
- log collection to a remote destination
- software upgrades

The basic steps to set dial-up as the primary connection are:

1. Create or assign an account with remote access privileges.
2. Create a dial-up interface, and enter the username of the account with remote access privileges as the dial-out username.
3. Create a static route for the dial-up interface, or assign a dial-out number, depending on the type of device selected.
4. Tell the application to use the route.

The following example demonstrates how to configure the dial-up interface.

Example: To configure SNMP auto trap dialout

Assign an account remote access privileges

1. Click **Configuration > Administrator Access > Accounts and Privileges > View by Accounts** tab.
2. Click **Add**.
   The **Add Account** dialog box appears. Refer to the *Administration Guide* (NN40020-600) for information on configuring an account.
3. Select the account to which you want to assign remote access privileges.
   The details panel appears.
4. Select the **Group Membership** tab.
5. Click **Add**.
   The **Add Account To Group** dialog box appears.
6. Select **Remote Access** group.
7. Click **OK**.

Create a dial-up interface

1. Click **Configuration > Resources > Dial Up Interfaces.**
2. Click **Add**.
   The **Add Interface** dialog box appears.
3. Select **Modem** from the drop-down menu.
4. Enter a logical name for the interface in the interface name field.
5. Click **OK**.
6. Select the new **Modem** interface.
7. Click the **Link Parameters** tab in the bottom panel.
8. Enter the **Dial-out number** to use for the back-up.
9. Click the **Access Parameters** tab in the bottom panel.
10. Select the account with remote access privileges from the **Dial-out user name** drop-down menu.
11. Select the **Authentication** value that is appropriate for your configuration. See Table 127 for a description of these fields.

Add the SNMP Trap destination

1. Click **Configuration > Administrator Access > SNMP > SNMP Trap Destinations** tab.
2. Click **Add**.
   The **Add Trap Destination** dialog box appears.
3. See the *Administration Guide* (NN40020-600) for information on how to configure the **Add Trap Destination** dialog box.

Note: The Host address must be the IP address of the static route created in this procedure.

4. Click **OK**.

Static Routes for Automatic Dial-out Interfaces

Static routes must be configured for Automatic Dial-out Interfaces. These can be programmed in Element Manager:

Configuration > System > IP Subsystem > Dial-Out Static Routes

Refer to “Configuring static routes” on page 463

Appendix A
VPN overview

A VPN (Virtual Private Network) is a group of systems connected across various data-transfer technologies that form a secure and private network.

BCM uses the Internet and tunneling protocols to create secure VPNs. These secure extranets require a protocol for safe transport from the BCM to another device through the Public Data Network (PDN). BCM uses the IPSec tunneling protocols.

Extranets can connect:

- mobile users to a fixed private network at their office over the PDN
- private networks in the two branch offices of the same corporation over PDN
- two divisions of the same corporation over the corporate intranet

When connecting two branch offices, the use of a VPN over the public data network is very efficient if the connection is required only intermittently or a dedicated point-to-point link is considered too expensive. Also, with the advent of business-to-business solutions, VPNs can be deployed to provide secure connections between corporations.

IPSec tunnels

In the IPSec Specification, there are two tunnel modes defined: tunnel mode and transport mode. BCM supports only tunnel mode. Tunnel mode describes a method of packetizing TCP/IP traffic to create a virtual tunnel.

Tunnels are created between servers, which are also known as gateways. This is called a Branch Office Connection. The end nodes connect to each other through gateways. These gateways set up the tunnel over the PDN on behalf of the end nodes. The establishment of the tunnel, and the PDN in between, is transparent to the end nodes which behave as if they are interacting through a router. Typically, the edge devices connecting the branches of a corporation to the ISP use VPN in this mode.

BCM is compatible with the Nortel Services Edge Router (formerly known as Shasta 5000) and the following versions of the Contivity VPN Client:

- V_05_01
- V_05_11
- V_06_01
- V_06_02
- V_07_01

The following describes configuring the tunnel portion of BCM using IPSec.

IPsec offers the following features:

- Branch Office support that allows you to configure an IPSec tunnel connection between two private networks.
- Support for IP address translation over encapsulation, packet-by-packet authentication.
- Strong encryption and token codes.

IPSec

Nortel and other third-party vendors support the IPsec tunneling protocol. IPsec is an emerging standard that offers a strong level of encryption (DES and Triple DES), integrity protection (MD5 and SHA), and the IETF-commended Internet Security Association & Key Management Protocol (ISAKMP) and Oakley Key Determination Protocols.

Encryption

All of the following encryption methods ensure that the packets have come from the original source at the secure end of the tunnel. Note that some of the encryption types will not appear on some non-US models that are restricted by US Domestic export laws.

Table 119 shows a comparison of the security provided by the available encryption and authentication methods.

Table 119 Comparing Encryption and Authentication Methods

Method (strongest to weakest)	Encryption of IP Packet Payload	Authentication of IP Packet Payload	Authentication of Entire IP Packet
ESP Triple DES SHA1	Yes	Yes	No
ESP Triple DES MD5	Yes	Yes	No
ESP 56-bit DES SHA1	Yes	Yes	No
ESP 56-bit DES MD5	Yes	Yes	No
ESP 40-bit DES SHA1	Yes	Yes	No
ESP 40-bit DES MD5	Yes	Yes	No
AH HMAC SHA1	No	No	Yes
AH HMAC MD5	No	No	Yes

Note: Using higher-level encryption, such as Triple DES, requires more system resources and increases packet latency. You must consider this when designing your overall network.

Note: If two devices have different encryption settings, the two devices will negotiate downward until they agree on a compatible encryption capability. For example, if Switch A attempts to negotiate Triple DES encryption with Switch B that is using 56-bit DES, then the Switch B will reject Triple DES encryption in favor of the 56-bit DES.

Each of the systems must have at least one encryption setting in common. If they do not, a tunnel is not negotiated. In the example above, both systems must have 56-bit DES enabled.

The encryption level you choose is made of three components:

- the protocol
- the encryption method
- the authentication method

Protocol

The protocol can be ESP or AH.

- ESP
  Encapsulating Security Payload (ESP) provides data integrity, source authentication and confidentiality for IP datagrams by encrypting the payload data to be protected. ESP uses the Data Encryption Standard (DES) and Triple DES algorithms.
- AH
  Authentication Header (AH) provides data integrity and source authentication. The AH method does not encrypt data.

Note: The use of a NAT device in the IPSec tunnel path can sometimes cause the AH method to report a security violation. This occurs because the NAT device changes the IP Address of an AH authenticated packet causing the authentication of this packet to fail.

Encryption method

The encryption method can be Triple DES, 56-bit DES or 40-bit DES. Triple DES is the strongest encryption and 40-bit DES is the weakest encryption.

- Triple DES
  Triple DES is an encryption block cipher algorithm that uses a 168-bit key. It uses the DES encryption algorithm three times. The first 56 bits of the key is used to encrypt the data, then the second 56 bits is used to decrypt the data. Finally, the data is encrypted once again with the third 56 bits. These three steps triple the complexity of the algorithm.
- 56-bit DES
  56-bit DES is an encryption block cipher algorithm that uses a 56-bit key (with 8 bits of parity) over a 64-bit block. The 56 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps.
- 40-bit DES
  40-bit DES is an encryption block cipher algorithm that uses a 40-bit key (with 8 bits of parity) over a 64-bit block. The 40 bits of the key are transformed and combined with a 64-bit message through a complex process of 16 steps. Both 40- and 56-bit DES require the same processing demands, so you should use 56-bit DES unless local encryption laws prohibit doing so.

Appendix B
Silence suppression

The following describes using silence suppression on half-duplex and full-duplex links:

Silence suppression, also known as voice activity detection, reduces bandwidth requirements by as much as 50 percent. The following explains how silence suppression functions on a Business Communications Manager network.

G.711 and G.729, support Silence suppression.

A key to VoIP Gateways in business applications is reducing WAN bandwidth use. Beyond speech compression, the best bandwidth-reducing technology is silence suppression, also known as Voice Activity Detection (VAD). Silence suppression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36% to 40% of a full-duplex conversation is active. When one person talks, the other listens. This is half-duplex. There are important periods of silence during speaker pauses between words and phrases. By applying silence suppression, average bandwidth use is reduced by the same amount. This reduction in average bandwidth requirements develops over a 20-to-30-second period as the conversation switches from one direction to another.

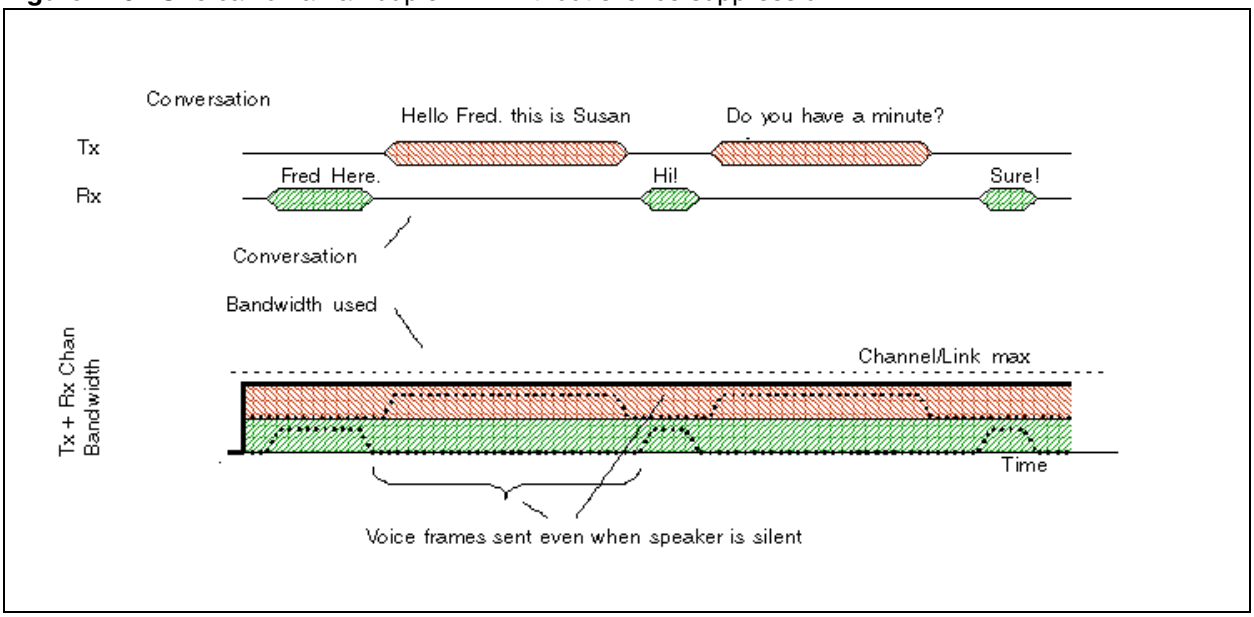
When a voice is being transmitted, it uses the full rate or continuous transmission rate.

The effects of silence suppression on peak bandwidth requirements differ, depending on whether the link is half-duplex or full-duplex.

Silence suppression on half-duplex links

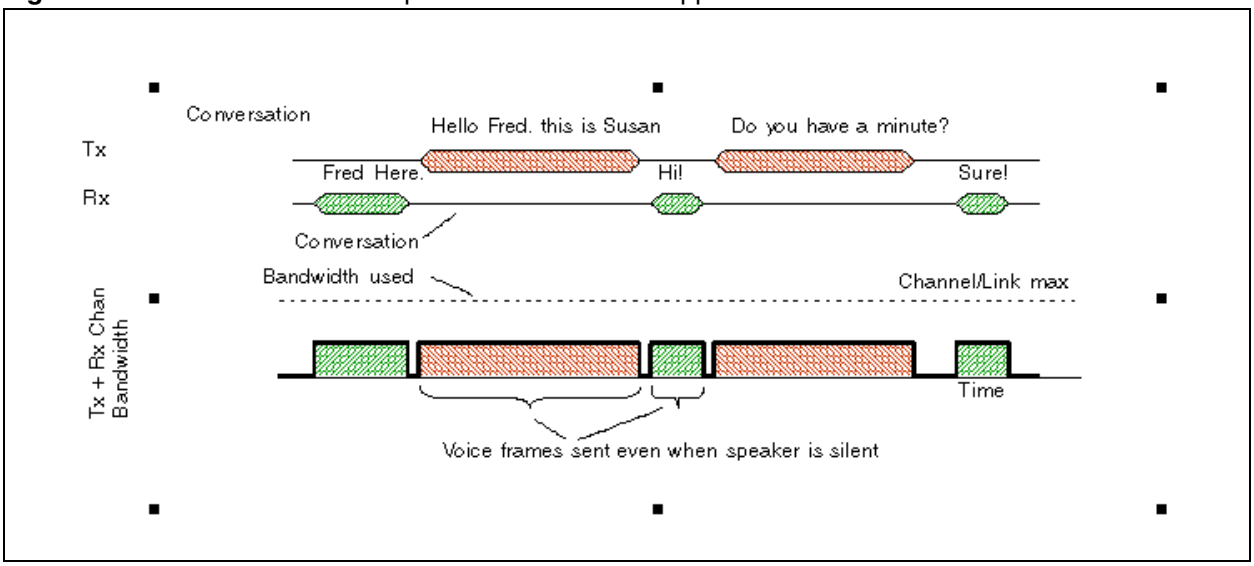
The following figure shows the bandwidth requirement for one call on a half-duplex link without silence suppression. Since the sender and receiver share the same channel, the peak bandwidth is double the full transmission rate. Because voice packets are transmitted even when a speaker is silent, the average bandwidth used is equal to the full transmission rate.

Figure 146 One call on a half-duplex link without silence suppression



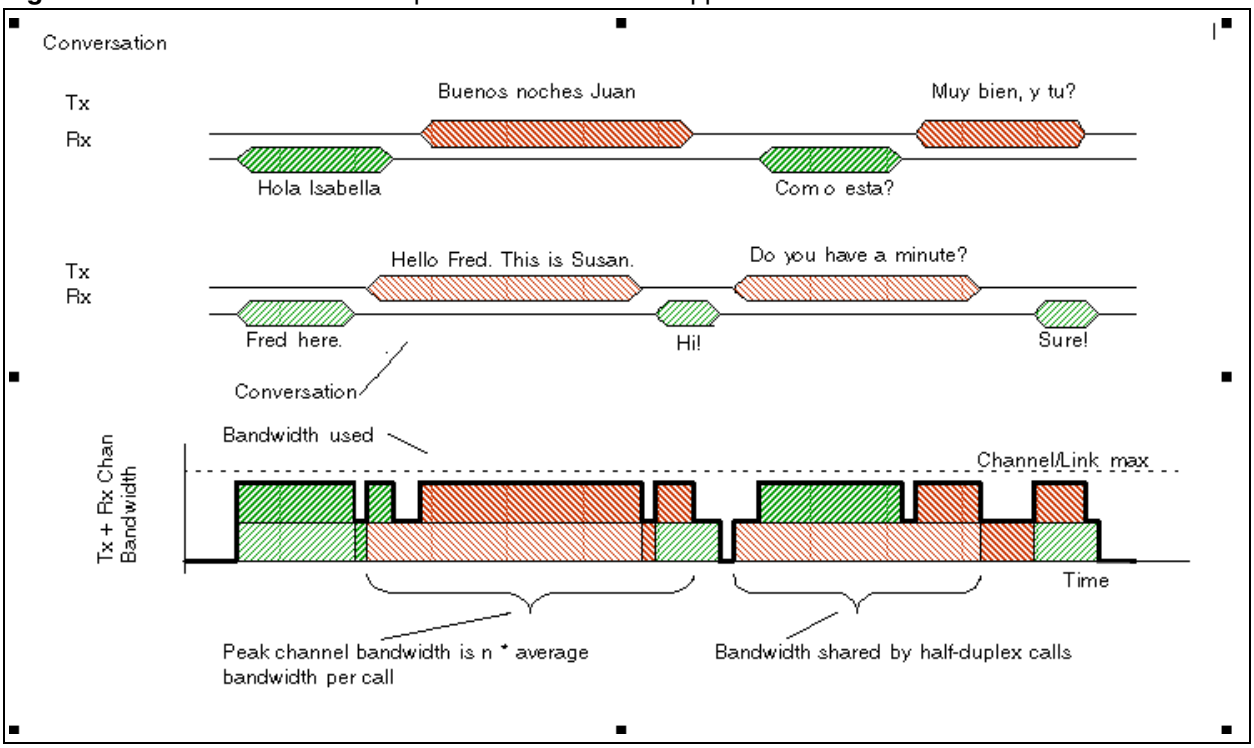
When silence suppression is enabled, voice packets are only sent when a speaker is talking. In a typical voice conversation, while one speaker is talking, the other speaker is listening – a half-duplex conversation. The following figure shows the peak bandwidth requirements for one call on a half-duplex link with silence suppression enabled. Because the sender and receiver alternate the use of the shared channel, the peak bandwidth requirement is equal to the full transmission rate. Only one media path is present on the channel at one time.

Figure 147 One call on a half-duplex link with silence suppression



The effect of silence suppression on half-duplex links is, therefore, to reduce the peak and average bandwidth requirements by approximately 50% of the full transmission rate. Because the sender and receiver are sharing the same bandwidth, this effect can be aggregated for a number of calls. The following figure shows the peak bandwidth requirements for two calls on a half-duplex link with silence suppression enabled. The peak bandwidth for all calls is equal to the sum of the peak bandwidth for each individual call. In this case, that is twice the full transmission rate for the two calls.

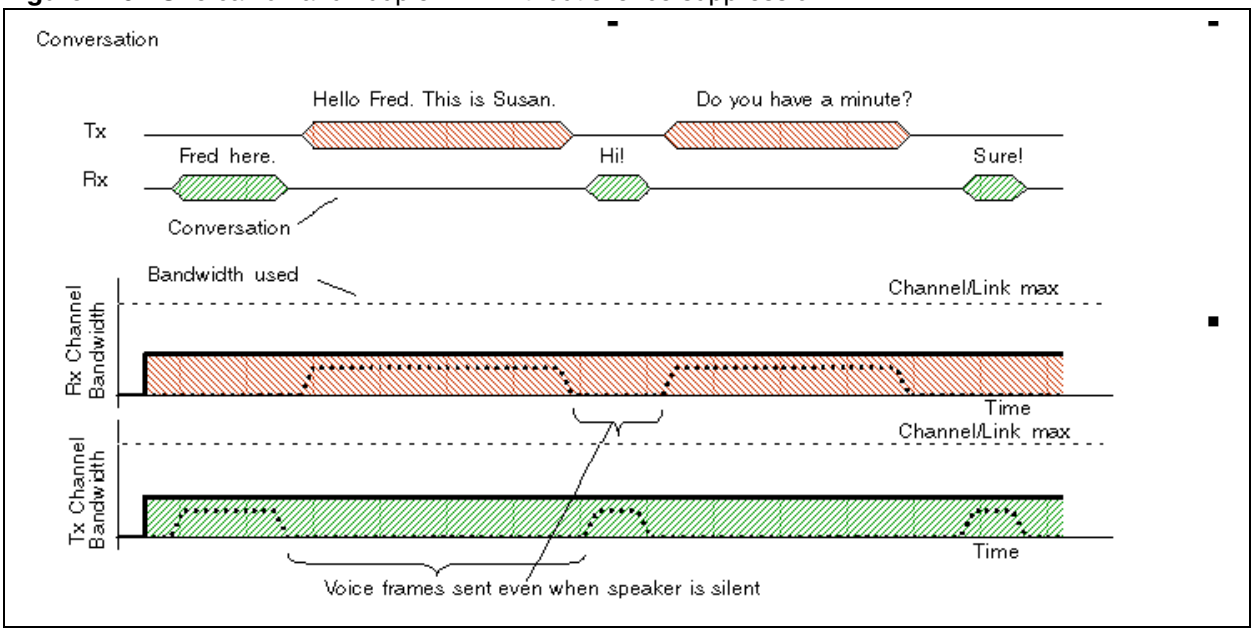
Figure 148 Two calls on a half-duplex link with silence suppression



Silence suppression on full-duplex links

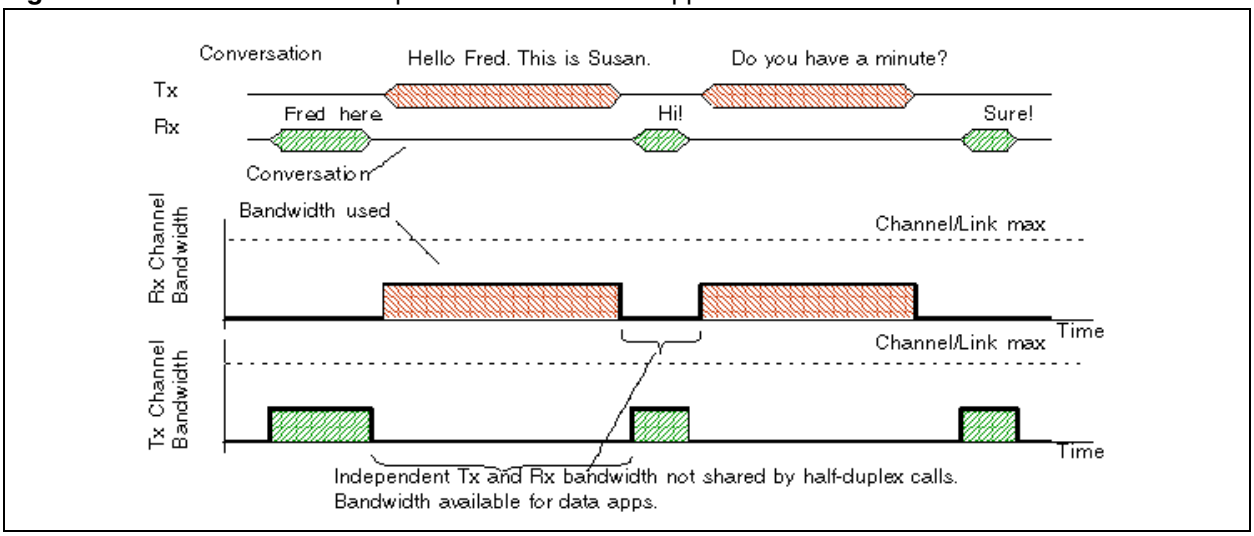
On full-duplex links, the transmit path and the receive path are separate channels, with bandwidths usually quoted in terms of individual channels. The following figure shows the peak bandwidth requirements for one call on a full-duplex link without silence suppression. Voice packets are transmitted, even when a speaker is silent. Therefore, the peak bandwidth and the average bandwidth used equals the full transmission rate for both the transmit and the receive channel.

Figure 149 One call on a full-duplex link without silence suppression



When silence suppression is enabled, voice packets are only sent when a speaker is talking. When a voice is being transmitted, it uses the full-rate transmission rate. Since the sender and receiver do not share the same channel, the peak bandwidth requirement per channel is still equal to the full transmission rate. The following figure shows the peak bandwidth requirements for one call on a full-duplex link with silence suppression enabled. The spare bandwidth made available by silence suppression is used for lower-priority data applications that can tolerate increased delay and jitter.

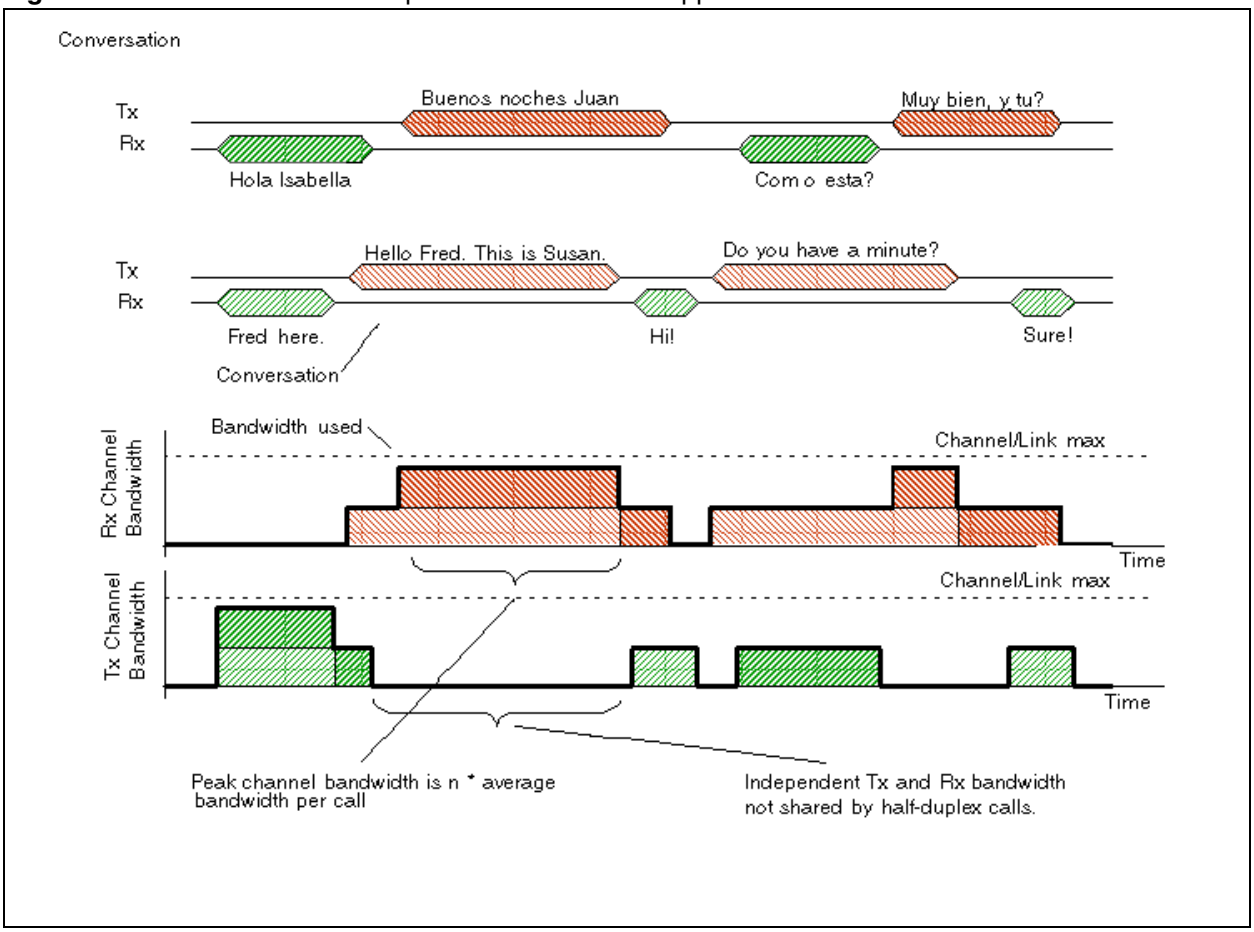
Figure 150 One call on a full-duplex link with silence suppression



When several calls are made over a full-duplex link, all calls share the same transmit path and they share the same receive path. Since the calls are independent, the peak bandwidth must account for the possibility that all speakers at one end of the link may talk at the same time. Therefore, the peak bandwidth for n calls is n * the full transmission rate. The following figure shows the peak bandwidth requirements for two calls on a full-duplex link with silence suppression. Note that the peak bandwidth is twice the full transmission rate, even though the average bandwidth is considerably less.

The spare bandwidth made available by silence suppression is available for lower priority data applications that can tolerate increased delay and jitter.

Figure 151 Two calls on a full-duplex link with silence suppression



Comfort noise

To provide a more natural sound during periods of silence, comfort noise is added at the destination gateway when silence suppression is active. The source gateway sends information packets to the destination gateway informing it that silence suppression is active and describing what background comfort noise to insert. The source gateway only sends the information packets when it detects a significant change in background noise.

Appendix C
ISDN overview

The following provides some general information about using ISDN lines on your BCM system. Detailed information about ISDN is widely available through the internet. Your service provider can also provide you with specific information to help you understand what suits your requirements.

Refer to the following:

- "Welcome to ISDN" on page 535
- "Services and features for ISDN BRI and PRI" on page 537
- "ISDN hardware" on page 542
- "ISDN standards compatibility" on page 545
- "Planning your ISDN network" on page 545
- "Supported ISDN protocols" on page 547

Welcome to ISDN

Integrated Services Digital Network (ISDN) technology provides a fast, accurate and reliable means of sending and receiving voice, data, images, text, and other information through the telecom network.

ISDN uses existing analog telephone wires and multiplex it into separate digital channels which increases bandwidth.

ISDN uses a single transport to carry multiple information types. What once required separate networks for voice, data, images, or video conferencing is now combined onto one common high-speed transport.

Refer to the following information:

- "Types of ISDN service" on page 536
- "ISDN layers" on page 536
- "ISDN bearer capability" on page 537

Analog versus ISDN

ISDN offers significantly higher bandwidth and speed than analog transmission because of its end-to-end digital connectivity on all transmission circuits. Being digital allows ISDN lines to provide better quality signaling than analog POTS lines, and ISDN out-of band data channel signaling offers faster call set up and tear down.

While an analog line carries only a single transmission at a time, an ISDN line can carry one or more voice, data, fax, and video transmissions simultaneously.

An analog modem operating at 14.4K takes about 4.5 minutes to transfer a 1MB data file and a 28.8K modem takes about half that time. Using one channel of an ISDN line, the transfer time is reduced to only 1 minute and if two ISDN channels are used, transfer time is just 30 seconds.

When transmitting data, the connect time for an average ISDN call is about three seconds per call, compared to about 21 seconds for the average analog modem call.

Types of ISDN service

Two types of ISDN services (lines) are available: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). Each line is made up of separate channels known as B and D channels which transmit information simultaneously.

- BRI is known as 2B+D because it consists of two B-channels and one D-channel.
- PRI is known as 23B+D(in North America) or as 30B+D (in Europe). In North America, 23B+D consists of 23 B-channels and one D-channel (T1 carrier). In Europe, 30B+D consists of 30 B-channels and one D-channel (E1 carrier).

B channels: B channels are the bearer channel and are used to carry voice or data information and have speeds of 64 kbps. Since each ISDN link (BRI or PRI) has more than one B-channel, a user can perform more than one transmission at the same time, using a single ISDN link.

D channels: The standard signaling protocol is transmitted over a dedicated data channel called the D-channel. The D-channel carries call setup and feature activation information to the destination and has speeds of 16 kbps (BRI) and 64 kbps PRI. Data information consists of control and signal information and for BRI only, packet-switched data such as credit card verification.

ISDN layers

ISDN layers refer to the standards established to guide the manufacturers of ISDN equipment and are based on the OSI (Open Systems Interconnection) model. The layers include both physical connections, such as wiring, and logical connections, which are programmed in computer software.

When equipment is designed to the ISDN standard for one of the layers, it works with equipment for the layers above and below it. Three layers are at work in ISDN for BCM. To support ISDN service, all three layers must be working properly.

- Layer 1: A physical connection that supports fundamental signaling passed between the ISDN network (your service provider) and the BCM system. When the LED on a BRI S/T Media Bay Module configured as BRI is lit, your layer 1 is functioning.
- Layer 2: A logical connection between the central office or the far end and the BCM system. BCM has one or two of these connections for each BRI link, and one for each PRI link. Without Layer 2, call processing is not possible.
- Layer 3: Also a logical connection between the ISDN network (your service provider) and the BCM system. For BRI lines, layer 3 is where call processing and service profile identifier (SPID) information is exchanged. This controls which central office services are available to the connection. For example, a network connection can be programmed to carry data calls.

Note: Throughout this chapter, references are made to Service profile identifiers (SPIDs). SPIDs are a part of the BRI National ISDN standard. SPIDs are not used in the ETSI BRI standard or on PRI.

The three layers mentioned in this section are important when you are installing, maintaining, and troubleshooting an ISDN system. For information about troubleshooting ISDN, see the *Administration Guide* (NN40020-600).

ISDN bearer capability

Bearer capability describes the transmission standard used by the BRI or PRI line so that it can work within a larger ISDN hardware and software network.

The bearer capability for BRI and PRI is voice/speech, 3.1 kHz audio (fax), and data (unrestricted 64 kbps, restricted 64 kbps, or 56 kbps).

Services and features for ISDN BRI and PRI

As part of an ISDN digital network, your system supports enhanced capabilities and features, including:

- faster call set up and tear down
- high quality voice transmission
- dial-up Internet and local area network (LAN) access
- video transmission
- network name display
- name and number blocking (PRI, BRI and analog)
- access to public protocols

Refer to the following features and services:

- "Network name display" on page 539
- "Name and number blocking (ONN)" on page 540
- "Call-by-Call Service Selection for PRI" on page 540
- "Emergency 911 dialing" on page 541
- "2-way DID" on page 541
- "Dialing plan and PRI" on page 541

PRI services and features

The services and features provided over PRI lines include:

- Call-by-call service selection (NI protocol)
- Emergency 911 dialing, internal extension number transmission
- access to Meridian 1 private networking (SL-1 protocol)

BRI services and features

The services and features provided over BRI lines include:

- data transmission at speeds up to 128 kbps per loop (depending on the bandwidth supported by your service provider)
- shared digital lines for voice and data ISDN terminal equipment

BCM Basic Rate Interface (BRI) also support D-channel packet service between a network and terminal connection. This allows you to add applications such as point-of-sale terminals (POSTA) without additional network connections. Connecting a POSTA allows transaction terminals (devices where you swipe credit or debit cards) to transmit information using the D channel of the BRI line, while the B channels of the BRI line remain available for voice and data calls. A special adapter links transaction equipment, such as cash registers, credit card verification rigs, and point-of-sale terminals, to the X.25 network, which is a data communications network designed to transmit information in the form of small data packets.

To support the D-packet service, your ISDN network and financial institution must be equipped with a D-packet handler. To convert the protocol used by the transaction equipment to the X.25 protocol, your ISDN network must also be equipped with an integrated X.25 PAD which works with the following versions of X.25: Datapac 32011, CCITT, T3POS, ITT and API. The ISDN service package you order must include D-packet service (for example, Package P in the United States; Microlink™ with D-channel in Canada).

Your service provider supplies a Terminal Endpoint Identifier (TEI) and DN to support D-packet service. The TEI is a number between 00 and 63 (in Canada, the default range is 21-63). Your service provider may also supply you with a DN to program your D-packet device. The DN for D-packet service becomes part of the dialing string used by the D-packet to call the packet handler.

Service provider features

BCM supports the following ISDN services and features offered by ISDN service providers:

- D-channel packet service (BRI only) to support devices such as transaction terminals. Transaction terminals are used to swipe credit or debit cards and transmit the information to a financial institution in data packets.
- Calling number identification (appears on both BCM sets and ISDN terminal equipment with the capability to show the information).
- Multi-Line hunt or DN hunting which switches a call to another ISDN line if the line usually used by the Network DN is busy. (*BRI only*)
- Subaddressing of terminal equipment (TE) on the same BRI loop. However, terminal equipment which supports sub-addressing is not commonly available in North America. (*BRI only*)

Transmission of B-channel packet data using nailed-up trunks is not supported by BCM.

Contact your ISDN service provider for more information about these services and features. For more information about ordering ISDN service in North America, see "Ordering ISDN PRI" on page 545 and "Ordering ISDN BRI" on page 546.

The terminal equipment (TE) connected to the BCM system can use some feature codes supported by the ISDN service provider.

Network name display

This feature allows ISDN to deliver the Name information of the users to those who are involved in a call that is on a public or private network.

Your BCM system displays the name of an incoming call when the name is available from the service provider. If the Calling Party Name has the status of *private* it may be displayed as `Private name` if that is how the service provider has indicated that it should be displayed. If the Calling Party Name is unavailable it may be displayed as `Unknown name`.

Your system might display the name of the called party on an outgoing call, if it is provided by your service provider. Your system sends the Business Name concatenated with the set name on an outgoing call but only after the Business Name has been programmed.

The available features include:

- Receiving Connected Name
- Receiving Calling Name

- Receiving Redirected Name
- Sending Connected Name
- Sending Calling Party Name

Consult your customer service representative to determine which of these features is compatible with your service provider.

Name and number blocking (ONN)

(North America only)

When activated, **FEATURE 819** allows you to block the outgoing name and/or number on a per-call basis. Name and number blocking can be used with a BCM set.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Call-by-Call Service Selection for PRI

(North America only)

PRI lines can be dynamically allocated to different service types with the Call-by-Call feature. PRI lines do not have to be pre-allocated to a given service type. Outgoing calls are routed through a dedicated PRI Pool and the calls can be routed based on various schedules.

The service types that may be available, depending on your service provider are described below:

- Public: Public service calls connect your BCM set with a Central Office (CO). DID and DOD calls are supported.
- Private: Private service calls connect your BCM set with a Virtual Private Network. DID and DOD calls are supported. A private dialing plan may be used.
- TIE: TIE services are private incoming and outgoing services that connect Private Branch Exchanges (PBX) such as BCM.
- FX (Foreign Exchange): FX service calls logically connect your BCM telephone to a remote CO. It provides the equivalent of local service at the distant exchange.
- OUTWATS: OUTWATS is for outgoing calls. This allows you to originate calls to telephones in a specific geographical area called a zone or band. Typically a flat monthly fee is charged for this service.
- Inwats: Inwats is a type of long distance service which allows you to receive calls originating within specified areas without a charge to the caller. A toll-free number is assigned to allow for reversed billing.

Consult your customer service representative to determine whether or not this feature is compatible with your provider.

Emergency 911 dialing

(North America only)

The ISDN PRI feature is capable of transmitting the telephone number and internal extension number of a calling station dialing 911 to the Public Switched Telephone Network (PSTN). State and local requirements for support of Emergency 911 dialing service by Customer Premises Equipment vary. Consult your local telecommunications service provider regarding compliance with applicable laws and regulations. For most installations the following configuration rules should be followed, unless local regulations require a modification.

- All PSTN connections must be over PRI.
- In order for all sets to be reached from a Public Safety Answering Position (PSAP), the system must be configured for DID access to all sets. In order to reduce confusion, the dial digits for each set should be configured to correspond to the set extension number.
- The OLI digits for each set should be identical to the DID dialed digits for the set.
- The routing table should route 911 to a PRI line pool.
- If attendant notification is required, the routing table must be set up for all 911 calls to use a dedicated line which has an appearance on the attendant console.
- The actual digit string 911 is not hard-coded into the system. More than one emergency number can be supported.

If transmission of internal extension numbers is not required or desired, Nortel recommends that the person in charge of the system maintain a site map or location directory so that emergency personnel can rapidly locate a BCM set given its DID number. Keep this list up-to-date and readily available.

IP telephony note: Ensure that you **do not** apply a 911 route to an IP telephone that is off the premises where the PSAP is connected to the system.

2-way DID

With PRI the same lines can be used for receiving direct inward dialing (DID) and for making direct outward dialing (DOD) calls.

The dialing plan configured by your customer service representative determines how calls are routed. Consult your customer service representative to determine whether or not this feature is compatible with your service provider.

Dialing plan and PRI

The Dialing Plan supports PRI connectivity to public and private networks. The dialing plan is a collection of features responsible for processing and routing incoming and outgoing calls. All PRI calls must go through a dialing plan.

Notes about the dialing plan:

- allows incoming calls to be routed to sets based on service type and digits received
- provides the ability to map user-dialed digits to a service type on a Call-by-Call basis
- allows long distance carrier selection through user-dialed Carrier Access Codes

Consult your customer service representative to determine how your dialing plan is configured.

ISDN hardware

To support connections to an ISDN network and ISDN terminal equipment, your BCM must be equipped with a BRI S/T Media Bay Module (BRIM) or a Digital Trunk Media Bay Module (DTM) card configured for PRI.

Refer to the following for a description of the BRI and PRI hardware:

- "PRI hardware" on page 542
- "BRI hardware" on page 542

PRI hardware

The Digital Trunk Media Bay Module (DTM) is configured for PRI. In most PRI network configurations, you need one DTM configured as PRI to act as the primary clock reference. The only time when you may not have a DTM designated as the PRI primary clock reference is in a network where your BCM system is connected back-to-back with another switch using a PRI link. If the other switch is loop-timed to your BCM system, your DTM (PRI) can be designated as a timing master.

If your BCM has more than one DTM configured as PRI, you must assign the first DTM as the primary external, the second DTM as the secondary reference.

BRI hardware

The loops on the BRI module can be programmed to support either network or terminal connections. This allows you to customize your arrangement of lines, voice terminals, data terminals, and other ISDN equipment. The following describes some basic hardware configurations for network and terminal connections for each loop type.

A BRI module provides four loops. Each loop can be individually programmed as:

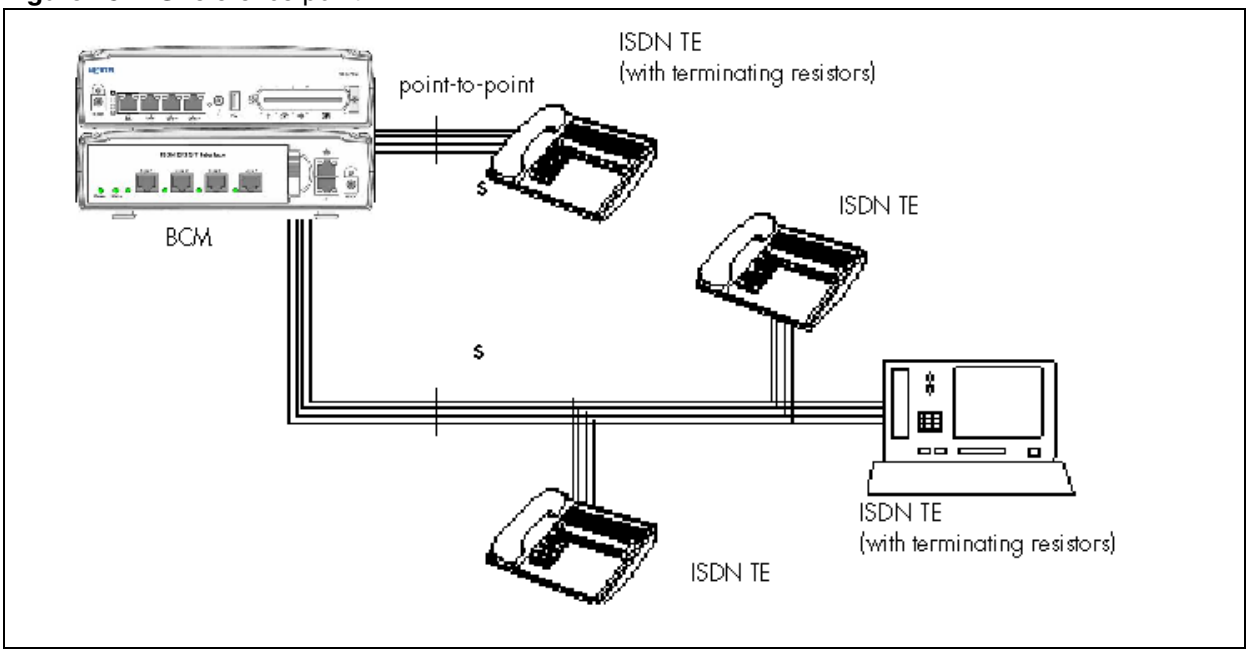
- an S reference point connection (S loop) to ISDN terminal equipment (TE), or
- a T or S reference point connection (T loop or S loop) to an ISDN network using an external NT1

S Reference Point

The S reference-point connection provides either a point-to-point or point-to-multipoint digital connection between BCM and ISDN terminal equipment (TE) that uses an S interface. Refer to Figure 152.

S loops support up to seven ISDN DNs, which identify TE to the BCM system.

Figure 152 S reference point

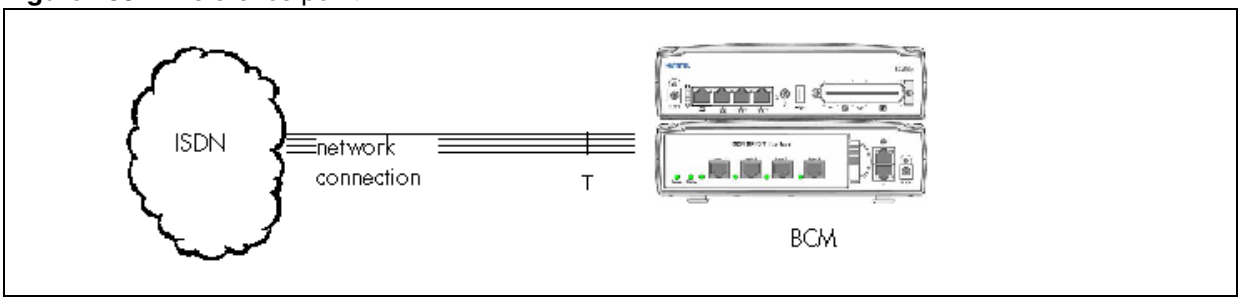


T Reference Points

The T reference-point connections provide a point-to-point digital connection between the ISDN network and BCM. Refer to Figure 153.

A T loop provides lines that can be shared by all BCM telephones, peripherals and applications, and ISDN TE.

Figure 153 T reference point



A T loop can be used in combination with an S loop to provide D-packet service for a point-of-sale terminal adapter (POSTA) or other D-packet device. D-packet service is a 16 kbps data transmission service that uses the D-channel of an ISDN line. The T and S loops must be on the same physical module.

Clock source for ISDN

Systems with ISDN interfaces need to synchronize clocking with the ISDN network and any ISDN terminal equipment connected to the network. Systems synchronize clocking to the first functionally available network connection. If there are excessive errors on the reference network connection, the next available network connection is used for clock synchronization. The clock synchronization process generates alarm codes and event messages. Clock synchronization is supported by the DTM, and BRI module

The BCM derives timing from the network using T reference points (loops). Terminal equipment on S reference points (loops) derive timing from the BCM system.

When you configure the network connections to the BCM, you should take into account the system preferences for selecting loops for synchronization:

- lower numbered loops have preference over higher numbered loops
- the loop preference order is: 201, 202, 203, 204 etc.
- the system skips S and analog loops, when selecting a network connection for synchronization

Systems with only S loops act as timing masters for the attached terminal equipment (TE), and are not synchronized to the network. ISDN TE without access to a network connection (BRI lines) has limited or no functionality.

If your system has both a BRI S/T configured as BRI, and a DTM configured as PRI, it is recommended that you use PRI as the primary clock source. See “PRI hardware” on page 542.

ISDN BRI NT1 equipment

The NT1 (network termination type 1) connects an S interface (four-wire) to a U interface (two-wire). In most cases, it connects loops from a BRI module to the network connection, which uses the U interface.

The NT1 converts and reformats data so it can be transmitted to and from the S or T connection. In addition, it manages the maintenance messages travelling between the network and the NT1, and between the NT1 and the BCM system.

The NT1 from Nortel is packaged two ways:

- a stand alone package which contains one NT1 card (NTBX80XX) and a power supply (NTBX81XX)
- a modular package which contains up to 12 NT1 cards (NTBX83XX) and a power supply (NTBX86AA)

ISDN standards compatibility

In North America, BCM ISDN equipment supports National ISDN standards for basic call and calling-line identification services. BCM BRI is compliant with National ISDN-1 and PRI is compliant with National ISDN-2.

BCM does not support EKTS (Electronic Key Telephone System) on PRI.

In Europe, BCM supports ETSI Euro and ETSI QSIG standards, and PRI SL-1 protocol.

Planning your ISDN network

Consult the*BCM50 2.0 Installation and Maintenance Guide* (NN40020-302) to determine a configuration of ISDN trunks and terminal equipment (TE) for the BCM system, and then order the appropriate ISDN capability package from your ISDN service provider.

For ISDN BRI service, your service provider supplies service profile identifiers (SPIDs), network directory numbers (Network DNs), terminal endpoint identifiers (TEIs), and other information as required to program your BCM, TE and other ISDN equipment.

BCM does not support any package with EKTS or CACH. EKTS is a package of features provided by the service provider and may include features such as Call Forwarding, Link, Three-Way Calling, and Calling Party Identification.

Ordering ISDN PRI

The following describes how to order ISDN PRI service for your BCM.

Ordering ISDN PRI service in Canada

Ordering ISDN PRI service in Canada/United States from your service provider. Set the BCM equipment to the PRI protocol indicated by your service provider.

Ordering ISDN PRI service outside of Canada and the United States

Outside Canada and the United States, order Euro ISDN PRI and/or BRI service from your service provider. Set the BCM equipment to the Euro ISDN protocol.

Ordering ISDN BRI

The following provides information about how to order ISDN BRI service for your BCM.

Ordering ISDN BRI service in Canada

In Canada, order Microlink™ service, the trade name for standard BRI service. You can order either regular Microlink™ service, which includes the CLID feature, or Centrex Microlink™, which includes access to additional ISDN network features, including Call Forwarding.

When ordering Microlink™ service, it must be ordered with EKTS turned off. If you will be using a point-of-sale terminal adapter (POSTA), ask for D-packet service to be enabled.

Ordering ISDN BRI service in the United States

In the United States, regardless of the CO (Central Office) type, order National ISDN BRI-NI-1 with EKTS (Electronic Key Telephone System) turned off. Use the following packages as a guideline for ordering your National ISDN BRI-NI-1. However, Nortel recommends using packages M or P with the BCM system. Contact your service provider for more information about the capability packages it offers. Bellcore/National ISDN Users Forum (NIUF ISDN packages supported by BCM (for ordering in U.S.).

	Capability	Feature set	Optional features	Point-of-sale	Voice	Data
M	Alternate voice/circuit-switched data on both B-channels	--	CLID	--	X	X
P	Alternate voice/circuit-switched data on both B-channels D-channel packet	flexible calling for voice (not supported by BCM) Basic D-Channel Packet	additional call offering (not supported by BCM) calling line identification	X	X	X

If you want to transmit both voice and data and support D-channel packet service, order package P. However, BCM does not support the flexible calling for voice and additional call-offering features that are included in package P.

Multi-Line Hunt may be ordered with your package. When a telephone number (the Network DN) in the group of numbers assigned by your service providers is busy, the Multi-Line Hunt feature connects the call to another telephone number in the group. BCM supports the feature only on point-to-point, network connections (T loop). Check with your service provider for more information about Multi-Line Hunt.

Any of the ISDN packages will allow you to use sub-addressing, but your ISDN TE must be equipped to use sub-addressing for the feature to work.

Ordering ISDN BRI service outside Canada or the United States

Outside Canada or the United States, order Euro ISDN PRI or BRI service, or both, from your service provider. Set the BCM equipment to the Euro ISDN protocol.

Supported ISDN protocols

The switch used by your service provider must be running the appropriate protocol software and the correct version of that software to support ISDN PRI and BRI. Each protocol is different and supports different services. Contact your service provider to make sure that your ISDN connection has the protocol you require.

Appendix D
Codec rates

The information in the table below enables the administrator to determine the number of resources that can be maintained on the available system bandwidth.

The packet transfer rate must also include the overhead.

Note: Using Silence Suppression on G.723 and G.729 can reduce the overall bandwidth consumption by 40%.

Note: The totals in the bytes/s column represent one direction only.

Table 120 RTP over IP (Sheet 1 of 2)

Payload (bytes)	Packets/frame	Overhead (bytes)	Total (bytes)	bytes/s	Overhead (%)	Latency (msec)
G.729						
10	1	58	68	54400	580.00	10
20	2	58	78	31200	290.00	20
***30**	**3**	**58**	**88**	**23467**	**193.33**	**30**
40	4	58	98	19600	145.00	40
50	5	58	108	17280	116.00	50
60	6	58	118	15733	96.67	60
70	7	58	128	14629	82.86	70
80	8	58	138	13800	72.50	80
90	9	58	148	13156	64.44	90
100	10	58	158	12640	58.00	100
G.711						
80	1	58	138	110400	72.50	10
160	2	58	218	87200	36.25	20
***240**	**3**	**58**	**298**	**79467**	**24.17**	**30**
320	4	58	378	75600	18.13	40
400	5	58	458	73280	14.50	50
480	6	58	538	71733	12.08	60
560	7	58	618	70629	10.36	70
640	8	58	698	69800	9.06	80
720	9	58	778	69156	8.06	90

Table 120 RTP over IP (Sheet 2 of 2)

Payload (bytes)	Packets/frame	Overhead (bytes)	Total (bytes)	bytes/s	Overhead (%)	Latency (msec)
800	10	58	858	68640	7.25	100
G.723						
24	3	58	82	21867	173.33	30
20	3	58	78	20800	160.00	30
Note: *These are the default values.						

Index

Numerics

2-way DID, PRI 541

4ESS
- available services 110
- call-by-call services support 237
- PRI protocol 239, 262

7100
- external code 269

A

absorbed length 242, 394, 395

access
- remote, public network 447

access codes
- default table 230
- line pool 234
- local access code 285
- national access code 285
- numbering
  - plan overview 218
- private access code 283
- programming 276, 282
- special (international) access code 285

adaptive, sampling 188

add
- automatic dial-out interface 522
- ISDN interface 503
- modem interface 508

advice of charge - end of call (AOCE), ETSI QSIG
- networking 52, 321

AH (authentication header)
- encryption protocol 528
- NAT restriction 528

alpha tagging 212

analog trunks
- module mode 104

ANI number, programming 136

answer
- backup, prime set for lines 132
- mode 136
- timer 105
- with DISA, trunk mode 133

answering calls
- call display services 214
- privacy 98

ANY character 251

ARS (automatic route selection). *See also* call routing 234

ASM (analog station module)
- Call Park prefix 231, 273

ATA2 (analog terminal adapter 2)
- Call Park prefix 231, 273
- external code 269

authentication header. *See* AH 528

auto DN
- overview 218

auto privacy, lines 135

auto-answer trunk
- DISA 420, 427
- private auto DN 282
- public auto DN 276
- remote restrictions 94
- T1 420, 427

autodial
- networks 249

automatic
- dial-out 497, 499
  - scheduled services 499
- dial-out interface 521
- keycode file upload 499
- software update pull 499

automatic CDR records push 499

B

background
- noise 533

backup answering
- prime set for lines 132

bandwidth
- available for other data 533
- silence compression 529

B-channels 536
- selection sequence 105
- sequence, ETSI QSIG networking 51, 314

BCM (Business Communications Manager)
- MCDN
  - private networking 297
  - system requirements 312
- network device prerequisites 466
- networking
  - MCDN with M1 43
  - multiple systems 327
- numbering plans overview 218
- overview 26

port settings 377
signaling method 383
system
configuration prerequisites 467
networking 294
tandem networking 36
using
a gatekeeper 378
firewalls 377
break-in, MCDN 301

BRI (Basic Rate Interface)
Answer with DISA 136
auto privacy 135
clock source 106, 544
full autohold 135
integrated 187
ISDN 536
mapping to target lines 132
module function 542
overlap receiving 189
programming 92
services and features 537
use auxiliary ringer 135
buffers, VoIP trunks 124, 127
busy tone
fast 425, 448
line settings 137
button programming
system speed dials 347
bypass call diversion 55, 331

C

call display
services 214
call diversion
bypass 55, 331
DPNSS 1 55, 331
follow-me 55, 332
immediate 55, 331
on busy 55, 331
on no reply 55, 331
call forward
DPNSS Embark switch 53, 332
maximum transits 106
call information
displaying information 214
call offer, DPNSS 58, 334
call park
analog telephones 231, 273
initiating (74) 230, 273
prefix 230, 273
call routing
tandem networks 44
call routing. *See also* ARS (automatic route selection) 234
call signaling, local gateway 120
call-by-call routing 238
call-by-call services
foreign exchange (FX) 236
International INWATS 236
INWATS 236
Nine hundred (900) 236
OUTWATS 236
PRI 540
private 236
public calls 236
routing table 238
service selection 108, 238
supporting protocols 148, 235
supporting switches 237
switched digital 236
Tie lines 236
calling outside 70, 99
calling party name display 212
CallPilot
DN length changes 224, 271
calls
making 399
originating in private network 326
within the system 70, 99
camp-on
MCDN 301
carrier access codes
code prefix 280
ID length 280
programming
long distance access 242, 256
Carrier Identification Code (CIC). *See* carrier access codes 234
CbC routing 344
CbC. *See* Call-by-Call services 344
CDP (coordinated dialing plan)
dialing plan 283
network dialing plan 398
private network
ID 283

MCDN 312
CDR (call detail recording)
records push
automatic 499
central administrator direct dial 269
channel characteristics
ISDN 505
Channel Service Unit. *See* CSU 108
channel, disable-enable a module port 87
Class of Service. *See* CoS 283
CLID
alpha tagging 212
match 212
name display 212
outgoing name and number blocking 210
overview 214
CLIR 210
clock source
ETSI QSIG networking 51, 314
ISDN 544
programming 106
code prefix, carrier access codes 280
comfort noise 533
compatibility
modem 500
computer, IP telephony prerequisites 468
conference
DPNSS 1 feature 54
configure
ISDN link parameters 507
modem link parameters 511
connect
ISDN interface 504
modem 509
connecting to system, remote dial-in 522
Contact Center
DN length change 224, 271
control set 131
setting the schedule 399
conventions, guide 28
button 28
buttons 28
command line 28
coordinated dialing plan. *See* CDP 283, 398
copyright 2
CoS (Class of Service)
auto DN 282
calls answered with DISA 276, 283
password, with DISA 420, 427
passwords 423, 443
programming 444
CSU (Channel Service Unit) 108

D

DASS2
clock source 106
if busy 137
received # 132
redirect to 137
use auxiliary ringer 135
data
encryption methods 527
networking
IPSec 527
D-channels 536
default
restriction filters 417, 436
delay
dial, signaling programming 134
delete
ISDN interface 504
modem interface 510
DES
encryption protocol 527
destination codes
absorbed length 242
ANY character 251
call-by-call services network 345
constraints 240, 243, 257, 264
dedicated long distance trunks 250
dialout to network 249
E&M networking 340
for fallback 393
least cost routing 243, 252
local calls 249
long distance access code routing 242, 256
MCDN network 310
numbering plan overview 218, 220
overflow routing 253
PSTN fallback 393
remote gateway destination digits 394, 395
schedule 394
wild card character 251
destination digits
destination code 394, 395
network example 398

remote gateway 385
destination gateway 533
destination IP
network example 398
remote gateway 385
DHCP (dynamic host configuration protocol)
IP telephone prerequisites 468
network prerequisites 466
dial
direct-dial telephones 231
mode
lines 133
signaling 134
tone
stuttered 425, 447
system 425, 447
dial tone
wait (804) 261
dial up
failover settings 512
interfaces 501
dialed digits, VoIP trunk routing 391
dial-in
ISDN 518
modem 501, 514
dialing
link code (F71) 261
long tones (F808) 261
pause (F78) 261
restrictions
maximum length 416
overrides 416
remote restrictions 418
wait for dial tone (F804) 261
dialing plan
CDP 312, 398
destination codes 255
destination digits 394, 395
line access diagram 228
location code, UDP 283
M1-IPT prerequisite 312
MCDN network checklist 303
outgoing
calls 385
private calls 287
public calls 223, 279
PRI 541
routing table 255
private
DN length 283
network ID 283
types 221
PSTN fallback 245, 374
public
DN lengths 221
lines 254
network 221
network code 277
public network
dialing plan 277
restriction filters 415, 433
system prerequisites 467
type 283
UDP 312
using T1 E&M lines 40
dial-out
automatic 497, 499, 521
add interface 522
disconnect interface 522
static routes 524
digits, destination codes 249
interfaces 501
local calls 249
modem 501
remote access 497
WAN failover 497
DID #, call-by-call service network 42, 343
DID (direct inward dialing)
ANI number 136
auto privacy 135
dial mode 133
redirect to 137
remote access 421, 430
signaling programming 134
system diagram 34, 290
use auxiliary ringer 135
digital
Answer with DISA 136
auto privacy 135
dial mode 133
redirect to 137
use auxiliary ringer 135
Digital Private Network Signaling System. *See* DPNSS 1 52
digital station module *See* DSM 106
Digital Trunk Interface. *See* DTI and DTM 39
direct dial
digit
Internal/External # (DN) 269
numbering overview 220

programming 269
type 269
digit facility 270
prime line 270
direct dial telephones 231
Direct Inward System Access. *See* DISA 283, 420, 427
DISA (direct inward system access)
DID, trunk 421, 430
DN
constraints 232, 273
overview 218
lines in a network 338
PRI trunks 431
private DISA DN programming 283
public DISA DN programming 276
remote access 420, 427
T1
DID trunks DISA DN 420, 427
E&M trunks 422, 432
VoIP trunks 367, 381
disable
a bus 87
ISDN interface 503
media bay module port 87
disabling
modem 509
disconnect
automatic dial-out interface 522
ISDN interface 504
modem 510
disconnect supervision
disconnect timer 106
loop start trunks 421, 430
display
network name 539
symbols 28
distinct ring. *See* DRP 132
distinctive ring pattern. *See* DRP 132
diversion
bypass call 55, 331
DPNSS 1 55, 331
follow-me 55, 332
immediate 55, 331
on busy 55, 331
on no reply 55, 331
DMS
private outgoing calls 287
DMS-100
available services 110
call-by-call services support 237
PRI protocol 239, 262
DMS-250
available services 110
call-by-call services support 237
PRI protocol 239, 262
DN
auto assign 467
changing the length 225, 271
disable-enable module port 87
hunting. *See* multi-line hunt 539
increasing length 224, 271
length
changing 224, 271
client application requirements 224, 271
numbering plan overview 218
overview 218
system startup 224, 270
voice mail/contact center 224, 271
records prerequisites 467
type
call-by-call services network 345
MCDN network 310
route programming 261
DNIS number 136
DPNSS (digital private network signaling system)
call offer 58, 334
diversion feature 55, 331
Embark switch 53, 332
full autohold 135
home location code 60, 335
host node 106
intrusion programming 57
networking 52
private access code 60, 335
protocol 37, 315
remote
access 421, 431
paging 422, 431
three-party service 54
use auxiliary ringer 135
DPNSS 1
call diversion 55, 331
features 53, 331
PBX link 52
terminating node 52
three party service 54
DRP (distinctive ring pattern) 132
DS/CLID, module mode 104
DSM (digital station module)

host node 106
DSX1 build 107
DTI trunk. *See also* DTM 39
DTM (digital trunk module)
clock source 544
ISDN hardware 542
DTMF (dual tone multi-frequency)
dial mode 133
setting ANI/DNIS 136

E

E&M
ANI number 136
answer timer 105
answer with DISA 136
auto privacy 135
dial mode 133
DNIS number 136
full autohold 135
redirect to 137
remote access issue 422, 432
signaling programming 134
use auxiliary ringer 135
Element Manager
destination codes 393
H.323
trunks record 385
Embark switch
DPNSS network 53, 332
host node 106
emergency
911 dialing, PRI 541
enable
a bus 87
ISDN interface 503
media bay module port 87
modem 509
encapsulating security payload. *See* ESP 528
encryption
DES 527
IPSec 527
levels 527
methods 527
Equal Access Identifier Code (CAC). *See* carrier codes 234
ESF (extended superframe)
framing format 107
ESP (encapsulating security payload)
encryption protocol 528
ETSI
name and number blocking 210
ETSI Euro
PRI protocol 239, 262
ETSI QSIG
advice of charge- end of call (AOCE) 52, 321
malicious call identification (MCID) 322
network
diversion 322
services 51, 321
networking 50, 313
PRI protocol 239, 262
private networking 37, 315
private outgoing calls 287
exception. *See* dialing restriction 416
extended superframe. *See* ESF 107
external # 394, 395
direct dial digit 269
E&M networking 340
route programming 261
external code
access codes 269
numbering overview 220
external lines
access code conflicts 232, 272
external routing feature codes 261
external voice mail
access programming 94

F

facility
direct dial programming 270
failover
dial up settings 512
ISDN interface 514
modem interface 514
WAN 500, 513, 514
fallback
activating VoIP schedule 395
configuring for PSTN 373
destination codes 393
MCDN 311
MCDN networking 312
scheduling 395
using PRI line 398
Fallback to circuit-switched 118, 125
fast busy tone 425, 448
fax over IP *See* FoIP 379

feature
68 - Class of Service (CoS) 447
74 - call park 230, 273
78 - 1.5-second pause 261
811 - call display 214
811 - call information 214
819 - outgoing name and number (ONN) blocking 540
features
link code (71) 261
long tones (808) 261
wait for dial tone code (804) 261
firewalls
configuring 377
network prerequisites 466
ports 377
first display 212
fixed, sampling 188
FoIP
T.38 401
FoIP (fax over IP) 379
follow-me diversion 55, 332
foreign exchange. *See* FX 540
framing format 107
full autohold 135
full duplex link, silence suppression examples 531
FX (foreign exchange)
call-by-call services 236
service, protocols 110

G

gatekeeper
defined 364
network prerequisites 465
signaling method 383
Gatekeeper IP, Local Gateway 120
gatekeeper IP, local gateway 384
GateKeeperResolved 120
GateKeeperRouted 120
gateway
destination digits 394, 395
network prerequisites 465
protocol 385
protocol, local gateway 384
remote, configuring 385
type 385
Gateway Protocol
Local Gateway 119
GATM (global analog trunk module)
module mode 104
global analog trunk module. *See* GATM 104
ground start
answer with DISA 136
auto privacy 135
dial mode 133
redirect to 137
use auxiliary ringer 135
GWProtocol 119, 384

H

H.323
endpoints 378
fallback setting 118
Fallback to circuit-switched 118
Trunks record
jitter buffer 124
trunks record
remote gateway 385
half duplex links
silence suppression example 529
home location code, DPNSS 60, 335
host node, DPNSS 106

I

ICL (intrusion capability level)
defined 57
ID length, carrier access codes 280
idle line, search for 97
IDPX, host node 106
if busy 137
impedance, lines 97
increasing DN length 224, 271
integrated
BRI 187
Integrated Services Digital Network. *See* ISDN 537
intercom
calls within the system 70, 99
prime line and direct dial telephones 270
interface
dial-out 501
ISDN 501
modem 501
interface levels 107
internal
CSU 108
direct dial digit 269

target line calls 91
Internal/External #, direct dial programming 269
international (special) access code 285
International INWATS, call-by-call services 236
Internet Security Association and Key Management Protocol (ISAKMP), IPSec 527
Intl-800 protocols 110
intranet
networking multiple BCMs 327
intrusion
DPNSS networking 57
Intrusion Capability Level. *See* ICL 57
Intrusion Protection Level. *See* IPL 57
INWATS
(800), protocols 110
call-by-call services 236
PRI 540
IP address
gatekeeper 383
ISDN 508
modem 512
network prerequisites 465
remote gateway 385
IP speech packets 124, 127
IP telephones
prerequisites 468
VLAN service 468
IP trunking
MWI remote capability 300
IP trunks
network prerequisites 465
IPL (intrusion protection level)
defined 57
IPSec
encryption protocols, ESP or AH 528
modes 525
NAT restriction 528
overview 527
ISDN (integrated services digital network)
911 dialing 541
add interface 503
B and D-channels 536
bearer capability 537
BRI card 542, 544
call-by-call services for PRI 540
capabilities 535
capability packages 545, 546
channel characteristics 505
clock source 544
clocking 544
compared to analog 536
configure link parameters 507
connect interface 504
data transmission speed 538
deleting an interface 504
dial-in parameters 518
dialing plan 541
digital access lines (DAL) settings 108
disable interface 503
disconnect interface 504
enable interface 503
hardware 542
interface 501
ISDN 502
IP address 508
layers 536
link parameters 506, 507
loss plan setting 107
network
name display 539
synchronization 544
ordering 545
ordering service 546
planning service order 536
PRI 2-way DID 541
programming sequence 92
remote access 498
S interface 543
S reference point 543
services and features 537, 539
standards 545
supported protocols 547
T reference point 543
terminal equipment configuration 543
type of services 536
ISDN call connection limitation (ICCL), MCDN 47, 320

J

jitter buffer
VoIP trunks 124, 127

K

keycode file upload
automatic 499
keycodes
MCDN networking 38, 315
prerequisite list 467
VoIP trunks 368

L

LAN
  Business Communications Manager function 467
least cost routing 243, 252
line access
  call diagram 228
  call-by-call services network 344
  MCDN network 310
line coding
  T1 parameters 107
line filter, CoS programming 444
line pool
  access code
    constraints 358
    programming 234
  network example 398
  numbering
    overview 220
    plan overview 218
  setting line type 131
  VoIP trunk routing 391
line programming
  ANI number 136
  answer mode 136
  answer with DISA 136
  auto privacy 135
  control set 131
  dial mode 133
  DNIS number 136
  full autohold 135
  if busy 137
  line type 131
  link at CO 134
  loss packages 97, 133
  name 131
  prime set 132
  private line 131
  public line 131
  received # 132
  redirect to 137
  restrictions 93
  signaling 134
  telco features 94
  trunk mode 133
  use auxiliary ringer 135
  use remote package 138
line type 131
line/set restrictions
  remote access, CoS 444
lines
  changing the name 213
  identifying 90
  numbering 39
  programming overview 98
  voice message center 137
link
  at CO, loop start analog lines 134
  code (F71) 261
  signal 134
link parameters
  ISDN 506, 507
  modem 510, 511
local
  access code
    MCDN 285
  calling routing 249
  calls
    destination codes 249
  e.164 outgoing calls 223, 279
local access code 285
local gateway
  Call Signaling 120
  gatekeeper
    IP 384
  Gatekeeper IP 120
  Gateway Protocol 119
  gateway protocol 384
  Registration TTL 121, 384
location code
  numbering overview 219
  UDP dialing plan 283
long distance
  call
    routes 250
    using CoS password 447
  dedicated trunks 250
long tones
  dialing code (F808) 261
loop
  disconnect timer 106
loop programming
  blocking state 188
  overlap receiving 189
  protocol 188
  sampling 188
Loop start
  redirect to 137
loop start

analog
auto privacy 135
digital
auto privacy 135
loop start analog
answer with DISA 136
dial mode 133
full autohold 135
link
at CO 134
loss packages 133
trunk mode 133
use auxiliary ringer 135
loop start digital
answer with DISA 136
dial mode 133
full autohold 135
trunk mode 133
use auxiliary ringer 135
loop start trunk
disconnect supervision, remote access 421, 430
remote access from public network 421, 430
loops
MWI PRI MCDN loops 106
loss packages, line programming 133
loss/gain settings 97

M

M1
PRI loops for MWI 106
M1, Host node 106
M1-IPT
gateway type 311
maintaining security 424, 446
maintenance
enabling the module 87
making calls, VoIP trunks 399
malicious call identification
ETSI network 322
maximum CLI per line 212
maximum length, dialing restrictions 416
maximum transits, transits
maximum 106
MCDN
break-in 301
PRI protocol 239
protocol 37
MCDN (Meridian Customer Defined Networking)
camp-on feature 301
CDP programming specifics 303
creating SL-1 or VoIP networks 356
DN types, routing 261
gateway type 311
ISDN call connection limitation (ICCL) 47, 320
local access code 285
M1-IPT requirements 312
media bay module settings 309
Meridian system requirements 297
message waiting indication (MWI) 299
national access code 285
network 46, 319
checklist 303
example 308
features 299
network call redirection information (NCRI) 46, 319
outgoing call display 261
over VoIP 311
PRI fallback 312
PRI M1 loops 106
private access code 283
private network ID 283
private networking 297
private outgoing calls 287
protocol 315
remote gateway 311
routing information 310
SL-1 networking 43
special (international) access code 285
special route codes 261
tandem calls 232, 257
trunk anti-tromboning (TAT) 49, 320
trunk route optimization (TRO) 48, 320
UDP programming specifics 303
Zone ID 286
media bay modules
clock source support 544
disable a bus 87
disable-enable a port 87
enable a bus 87
MCDN network settings 309
task list 81
menu
lines 90
Meridian
MCDN network 46, 319
MCDN system requirements 297
Meridian (Meridian Customer Defined Networking)
SL-1 networking 43
Meridian 1

M1-IPT 368
MCDN
special calls 232, 257
MCDN networking 311
message waiting indication
MCDN 299
messages
network features 299
modem
add interface 508
compatibility 500
configure IP address 512
connecting 509
delete interface 510
dial-in 501, 514
dial-out 501
disabling 509
disconnect 510
enabling 509
interface 501, 508
IP address 512
link parameters 510, 511
remote access 498, 499
modify
ISDN channel characteristics 506
module
networking 39
module mode
module record 104
multi-line hunt 539, 546
MWI
M1 remote capability 106, 300
MWI M1 106

N

N1
call-by-call services 540
name
blocking, ONN 540
changing, telephony 213
lines 131
network display 539
remote gateway 385
name display
calling party 211
network 211
selective line redirection 212
name display, alpha tagging 212
NAT (network address translation)
IPSec restriction 528
NAT, network prerequisites 466
national
e.164 outgoing calls 223, 279
national access code 285
MCDN 285
National ISDN standards 545
Netmask
network prerequisites 465
network
autodial access 249
devices, prerequisites 466
dial-out digits 249
locations, prerequisites 465
port settings 377
private systems to BCM 37, 294
public network to BCM 37, 294
T1 E&M 40, 339
network #
call-by-call service network 42, 343
ETSI QSIG 50, 313
MCDN 308
networking 40, 339
network call redirection information (NCRI), MCDN 46, 319
network diversion, ETSI network 322
network name display 539
calling party name 212
General heading 211
selective line redirection (SLR) 212
networking
advice of charge - end of call (AOCE) feature 52, 321
Business Communications Manager prerequisites 467
destination code 340
DPNSS 1 52
features 53
DPNSS 1 three party service 54
DPNSS connected to Embark 53, 332
E&M remote access 340
E&M routing destinations 340
E&M routing service 340
ETSI QSIG 50, 313
ETSI QSIG services 51, 321
external # 340
keycodes 38, 315
malicious call identification (MCID) 322
MCDN

private networking 297
MCDN check list 303
MCDN features 299
MCDN network example 308
MCDN over VoIP 311
MCDN routing 310
MCDN Zone ID for SRG 286
MCDN, break-in 301
MCDN, camp-on feature 301
MCDN, ISDN call connection limitation (ICCL) 47, 320
MCDN, message waiting indication (MWI) 299
MCDN, network call redirection (NCRI) 46, 319
MCDN, trunk anti-tromboning (TAT) 49, 320
MCDN, trunk route optimization (TRO) 48, 320
media bay module settings 309
Meridian MCDN system requirements 297
multiple BCMs 327
network # 40, 339
network diversion 322
node 43, 323
programming MCDN 356
protocols 37, 315
PSTN fallback 373
received # 40, 339
restriction filters 41, 342
signaling method 383
system callers 36, 294
tandem network 325
tandem network originating calls 326
tandem network routing 44
UDP and CDP programming 303
using T1 E&M lines 40
Virtual Private Network ID 286

networks
DPNSS 1 53
MCDN 46, 319
VLAN ports 468

NI
call-by-call services support 237
loop programming protocol 188
PRI protocol 239, 262

NI-2, available services 110

Nine hundred (900)
call-by-call services 236
protocols 110

node
tandem network 43, 323
terminating, DPNSS 1 52

NSF Extension 105

NT1 (network termination type 1) 544

numbering plans, overview 218

O

Oakley Key Determination Protocols 527

OLI
changing DN length 225, 271

ONN (outgoing name and number) blocking
feature 819 540

ONN blocking
state 188

open switch interval (OSI) 133

outgoing
call configuration 385
call display
MCDN 261
name and number blocking 210
private network calls 287
public network calls 223, 279

outgoing calls 385

Outwats
PRI 540

OUTWATS, call-by-call services 236

overflow routing 243, 252
VoIP fallback routing 244, 253

overflow setting 395

overlap receiving 189

overrides
dialing restrictions 416

P

page
remote 422, 431

park prefix
numbering overview 220
SWCA 269

park prefix, access codes 269

parked call
retrieving 269

password
calls answered with DISA 276, 283
CoS 423, 443
CoS programming 444
using DISA 420, 427

pause
insert into dialing sequence (F78) 261

PBX

DPNSS 1 networking 52
system diagram 33, 289
port
disable-enable 87
port settings 377
ports
firewalls 377
legacy networks 377
preferred codec 123, 126
prerequisites
IP telephones 468
keycodes 467
M1-IPT MCDN 312
network devices 466
system configuration 467
PRI
private networking 37, 297
SL-1 networking 319
PRI (Primary Rate Interface)
911 dialing 541
available services, per protocol 110
B-channel selection sequence 105
call-by-call service selection 108
call-by-call services 148, 235
clock source 106
dialing plan routing table 255
ETSI QSIG hardware settings 51, 314
hardware 542
ISDN 536
MCDN fallback 312
MCDN network dialing 283
MWI remote capability, MCDN 300
NSF extension 105
private networking 315
protocol 105
protocol type 105
remote access 431
remote access, Auto DN or DISA DN 422, 432
services and features 537
SL-1 networking 46
target line busy tone 137
prime line
direct dial telephone 270
prime telephone
lines 132
Privacy
changing status 98
private access code 283
DPNSS 60, 335
private auto DN 282
DN received number lengths 232, 272
private DISA DN
received number lengths 232, 272
Private DN length
numbering overview 219
private DN length, UDP dialing plan 283
private DN, route programming 261
private IP address 466
Private length
received # 276
private line 131
Private name 212
private network
advice of charge - end of call (AOCE) feature 52, 321
callers 37, 294
calls originating in tandem network 326
dialing plan type 283
DPNSS 1 features 53
DPNSS 1 three party service 54
ETSI QSIG 50, 313
services 51, 321
MCDN 297
camp-on feature 301
ISDN call connection limitation (ICCL) 47
message waiting indication (MWI) 299
network call redirection information (NCRI) 46, 319
routing information 310
trunk anti-tromboning (TAT) 49, 320
trunk route optimization (TRO) 48, 320
MCDN (Meridian Customer Defined Networking)
break-in 301
MCDN ISDN call connection limitation (ICCL) 320
Meridian MCDN requirements 297
private DN length 283
private network ID 283
remote access 38, 316, 422, 432
UDP location code 283
private network ID
numbering overview 219
private network ID, dialing plan 283
private network, MCDN Zone ID 286
private network, virtual ID 286
private networking
MCDN
private access code 283
special calls 257

MCDN (Meridian Customer Defined Networking)
special calls 232
MCDN special route codes 261
outgoing calls 287
private services call 540
private, call-by-call services 236
process map
access headings 427, 439
programming
ISDN BRI 92
lines 90
protocol
ISDN supported 547
loop programming 188
PRI lines 105
remote gateway 385
protocols
T.38 401
PSTN (public switched telephone network)
analog access lines (AAL) settings 108
PSTN fallback 373, 384
activating VoIP schedule 395
configuring 373
destination codes 393
dialed digits 391
MCDN networking 312
PRI line 398
scheduling 395
public auto DN 276
DN received number lengths 232, 272
public data network, see PDN 525
public DISA DN
received number lengths 232, 272
public DN length
setting 221
Public DN lengths
numbering overview 219
Public DN, route programming 261
public IP address 466
public length
received # 276
public line 131
public network
callers 37, 294
code 277
dialing plan 254
dialing plan programming 221
public DN lengths 221
public network code 277
public network plan 277
to tandem network 325
public network dialing plan 277
public networking
outgoing calls 223, 279
public service calls 540
Public, call-by-call services 236

Q

QoS
MCDN networking 312
QoS monitor
enabled 398
remote gateway 385
QSIG
loop programming protocol 188
private networking 37, 315

R

receive threshold 385, 398
Received #
overview 218
received #
call-by-call service network 42, 343
ETSI QSIG 50, 313
line configuration 132
MCDN 308
networking 40, 339
received # length
programming 276
received number lengths
auto DNs 232, 272
DISA DNs 232, 272
redirect to, line programming 137
Registration TTL, Local Gateway 384
Registration TTL, Local gateway 121
regulatory information 2
related publications 29
remote
system access 420
remote access
CoS passwords 423, 443
dial out 497
DPNSS 421, 431
E&M networking 340
from public network 421, 430
IP trunks, no tone 425, 448

ISDN 498
loop start trunks 421, 430
modem 498, 499
numbering overview 218
package, CoS programming 444
PRI 422, 432
PRI trunk 431
private auto DN 282
private DISA DN 283
private network 38, 316, 422, 432
programming 444
public auto DN 276
public DISA DN 276
T1 DID trunk 421, 430
T1 E and M trunks 421, 430
using DISA 420, 427
VoIP trunks 422, 432
remote access, VoIP trunks 371, 372
remote capability, MWI 106, 300
remote dial-in 522
remote dial-in, guidelines 522
remote gateway
configuring 385
MCDN networking 311
network example 398
VoIP trunks 385
remote paging 422, 431
remote restrictions
dialing restrictions 418
remote access, CoS 444
VoIP trunks 422, 432
remote system, VoIP trunks 367, 381
restriction filters
default filters 417, 436
lines 416
networking 41, 342
programming 415, 433
remote access 416
removing 416
services 415
telephones 416
restrictions
line filter, CoS 444
lines 93
retrieving
call park 230, 273
route programming
DN type 261
external # 261
private DN 261
public DN 261
Use pool 261
router
port settings 377
routing 242, 256
call-by-call routing table 238
call-by-call services network 344
CbC services routing 344
dedicated trunks for long distance 250
defining multiple routes 243, 252
destination codes 255
destination wild card character 251
destinations, E&M networking 340
least cost routing 243, 252
local calling 249
long distance access code 242, 256
long distance calling 250
MCDN network 310
MCDN private network 310
network example 399
overflow programming 243, 252
PRI routing table 255
PSTN fallback 395
public network dialing 254
service, E&M networking 340
service, MCDN network 310
tandem networks 44
VoIP trunks 391

S

S interface 543
S loop, sampling programming 188
S or T reference point 543
S reference point 543
schedule
activating VoIP schedule 395
control set 399
destination codes 394
PSTN fallback 395
service setting, manual 395
scheduled services
automatic dial-out 499
SCNFallback 120
security
dialing restriction 415, 433
IPSec 527
recommendations, remote access 424, 446
remote access on VoIP trunks 422, 432
See ISDN

Selective LIne Redirection, see SLR 212
service code
North American ONN blocking 210
service code, ONN blocking 188
service selection 108
service setting, manual 395
service type
call-by-call network 344
services
restriction filters 415
routing 344
set restrictions
remote access, CoS 444
SF (superframe)
framing format 107
signaling
dial mode 133
line programming 134
signaling method 383
silence suppression
about 529
comfort noise 533
full duplex 531
half duplex 529
SIP
fallback setting 125
Fallback to circuit-switched 125
Trunks record
jitter buffer 127
SL-1
ETSI QSIG networking 50, 313
Gateway Protocol 119
gateway protocol 384
MCDN example 308
MCDN fallback 312
MCDN network 46, 319
PRI protocol 262
private networking 38, 315
SLR, calling and connected name display 212
software update pull
automatic 499
source gateway 533
special
outgoing calls 223, 279
special (international) access code 285
speech packets, silence suppression 529
speed dial
system codes 347
square system 33
SRG
MCDN Zone ID 286
Virtual Private Network ID 286
Start DN
overview 218
static routes
automatic dial-out 524
stuttered dial tone 425, 447
Succession
MCDN Zone ID 286
Virtual Private Network ID 286
superframe 107
supervised trunk mode 133
suppression bit 188, 210
SWCA
park prefix 269
switched digital
(SDS) protocols 110
call-by-call services 236
switches
call-by-call services support 237
synchronize clock source 544
system
dial tone 425, 447
system access
remote 420
system configuration, Business Communications Manager prerequisites 467
system speed dial
alpha tagging 212
codes (01-70) 347
system startup
DN length 224, 270
system-wide dialing, direct-dial telephones 231

T

T reference point 543
T.38 fax 379
enabling 401
T1
answer timer 105
clock source 106
DID trunk, remote access 421, 430
DID trunks, DISA DN 420, 427
disconnect timer 106

E&M network diagram 40
E&M private networking 37, 315
full autohold, E&M 135
parameters
DSX1 build 107
framing 107
internal CSU 107, 108
line coding 107
signaling tone setting 133
tandem calls
MCDN
special labels 257
MCDN (Meridian Customer Defined Networking)
special labels 232
tandem networking
call routing 44
from public network 325
target lines
BRI auto-answer trunk mapping 132
changing DN length, affecting received number 225, 271
changing the name 213
description 39
if busy 137
programming 91
received # 132
redirect to 137
use auxiliary ringer 135
TE (see ISDN terminal equipment) 543
telco features
programming lines 94
telephone programming
changing the name 213
direct dial 269
increasing DN length 224, 271
received # length 276
system speed dial 347
telephony services
DID system 34, 290
PBX, system diagram 33, 289
square system 33
terminating node, DPNSS 1 52
three party service, DPNSS 1 54
Tie lines
call-by-call services 236
DN type 261
Tie services 540
TimeToLive 384
tone
IP trunks, remote access 425, 448
remote access tones 425, 447
trademarks 2
Transmit Threshold 385, 398
transport mode, IPSec 525
trunk
DTM 39
mode 133
numbering 39
types 39
trunk anti-tromboning (TAT), MCDN 49, 320
trunk modules
line type 83
trunk route optimization (TRO), MCDN 48, 320
trunk/line data
call-by-call services network 344
MCDN network 310
TTL (TimeToLive) 121
tunnel mode, IPSec 525
tunneling
encryption methods 527
IPSec 527
type
direct dial 269

U

UDP (universal dialing plan)
dialing plan 283
dialing plan location code 283
port ranges 377
private DN lengths 283
private network ID 283
private network, MCDN 312
Unified Messaging 327
universal dialing plan*See* UDP and dialing plan 283
Unknown name 212
unsupervised trunk mode 133
Use pool, routing 261
use remote package 138
user filter
restrictions 444
using your system remotely 447

V

VAD (Voice Activity Detection)
silence suppression 529
Vertical Service Code (VSC) 210

Virtual Private Network ID 286
virtual private networks, see VPN 525
VLAN
  i-series telephones 468
Voice Activity Detection *See* VAD 529
Voice Activity Detection. *See* VAD 529
voice jitter buffer 124, 127
voice mail
  DN length change 224, 271
  setting remote access for lines 137
voice message center
  line setting 137
  programming 94
VoIP
  auto privacy 135
  DISA 367, 381
  fallback routing 244, 253
  full autohold 135
  gateway, prerequisites 465
  private networking 37, 315
  schedule, activating 395
  schedule, setting up 395
  use auxiliary ringer 135
VoIP trunks
  activating VoIP schedule 395
  destination codes 393
  jitter buffer 124, 127
  keycodes 368
  making calls 399
  MCDN private outgoing calls 287
  networking multiple systems 327
  outgoing call configuration 385
  outgoing calls 385
  overview 99
  port ranges, legacy systems 377
  port settings 377
  PSTN fallback 373
  PSTN fallback schedule 395
  remote access issues 422, 432
  remote access warning 371, 372
  remote gateway 385
  routing 391
  signaling method 383
  using firewalls 377
  voice activity detection 124, 127
VoIP trunks, configuring 367, 381
VoIP trunks, T.38 fax protocol 379
VSC 210

W

Wait for dial tone (804) 261
WAN
  Business Communications Manager function 467
  failover 500, 513
    dial-out interface 497
    ISDN 514
    modem 514
wild card character
  Destination codes ANY character 251
WinkStart 134
workstation prerequisites 468

Z

zone ID
  MCDN 286